STIC Search Report
EIC 1700

STIC Database Tracking Number: 110615

TO: Aravind K Moorthy
Location: 4B14
Art Unit : 2131
December 23, 2003

Case Serial Number: 09/596924

From: Terese Esterheld
Location: EIC 2100
CPK2 4B30
Phone: 308-7795

Terese.Esterheld@uspto.gov

Search Notes

Dear Examiner Moorthy,

I have searched Encryption or Cryptographic Service, Pricing, Computational Burden, Privacy Level and Speed.

I found patents that contain parts of your request.

Please look over the complete package as there may be articles not marked that are of value to you.

If I can be of further assistance with this search, please let me know.

Terese Esterheld

sira
Search and Information Resources Administration

```
Set     Items   Description
S1       5899   AU=(BERSON, T? OR BERSON T? OR DEAN, R? OR DEAN R? OR FRAN-
             KLIN, M? OR FRANKLIN M? OR LUNT,, T? OR LUNT T? OR SMETTERS, -
             D? OR SMETTERS D?)
S2          2   S1 AND (ENCRYPTION OR CRYPTOGRAPHIC)()SERVICE?
File   2:INSPEC 1969-2003/Dec W1
         (c) 2003 Institution of Electrical Engineers
File   6:NTIS 1964-2003/Dec W3
         (c) 2003 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2003/Dec W2
         (c) 2003 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2003/Dec W3
         (c) 2003 Inst for Sci Info
File  35:Dissertation Abs Online 1861-2003/Nov
         (c) 2003 ProQuest Info&Learning
File  65:Inside Conferences 1993-2003/Dec W3
         (c) 2003 BLDSC all rts. reserv.
File  92:IHS Intl.Stds.& Specs. 1999/Nov
         (c) 1999 Information Handling Services
File  94:JICST-EPlus 1985-2003/Dec W3
         (c)2003 Japan Science and Tech Corp(JST)
File  95:TEME-Technology & Management 1989-2003/Nov W5
         (c) 2003 FIZ TECHNIK
File  99:Wilson Appl. Sci & Tech Abs 1983-2003/Nov
         (c) 2003 The HW Wilson Co.
File 103:Energy SciTec 1974-2003/Dec B1
         (c) 2003 Contains copyrighted material
File 144:Pascal 1973-2003/Dec W2
         (c) 2003 INIST/CNRS
File 202:Info. Sci. & Tech. Abs. 1966-2003/Nov 17
         (c) 2003 EBSCO Publishing
File 233:Internet & Personal Comp. Abs. 1981-2003/Jul
         (c) 2003, EBSCO Pub.
File 239:Mathsci 1940-2003/Jan
         (c) 2003 American Mathematical Society
File 275:Gale Group Computer DB(TM) 1983-2003/Dec 23
         (c) 2003 The Gale Group
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File 647:CMP  Computer Fulltext 1988-2003/Dec W3
         (c) 2003 CMP Media, LLC
File 674:Computer News Fulltext 1989-2003/Dec W1
         (c) 2003 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2003/Dec 22
         (c) 2003 The Dialog Corp.
?
```

```
T S2/5/ALL

  2/5/1     (Item 1 from file: 2)
DIALOG(R)File   2:INSPEC
(c) 2003 Institution of Electrical Engineers. All rts. reserv.

6887599   INSPEC Abstract Number: B2001-05-6120D-032, C2001-05-6130S-037
  Title: Cryptography everywhere
  Author(s): Berson, T.A.
  Author Affiliation: Anagram Labs., Xerox Palo Alto Res. Center, CA, USA
  Conference Title: Advances in Cryptology - ASIACRYPT 2000. 6th
International Conference on the Theory and Application of Cryptology and
Information Security. Proceedings (Lecture Notes in Computer Science
Vol.1976)   p.72
  Editor(s): Okamoto, T.
  Publisher: Springer-Verlag, Berlin, Germany
  Publication Date: 2000  Country of Publication: Germany    xii+630 pp.
  ISBN: 3 540 41404 5     Material Identity Number: XX-2001-00244
  Conference Title: Advances in Cryptology - ASIACRYPT 2000. 6th
International Conference on the Theory and Application of Cryptology and
Information Security
  Conference Sponsor: Int. Assoc. Cryptologic Res. (IACR); IEICE
  Conference Date: 3-7 Dec. 2000    Conference Location: Kyoto, Japan
  Language: English    Document Type: Conference Paper (PA)
  Treatment: General, Review (G)
  Abstract: Summary form only given. The past twenty years have seen
cryptography move from arcane to commonplace, from difficult to easy, from
expensive to cheap. Many influences are at work. These include: the
professionalization of cryptographers, in which the IACR has played a
significant role; the creation of textbooks and of courses; the steady
growth of computational power delivered by the operation of Moore's law;
the algorithmic advances made by cryptographic researchers and engineers;
the rise of E-commerce and wireless infrastructures which have a seemingly
endless appetite for cryptographic services; the entry of many young people
into the field; and the easing of government export controls. We envisage a
near future where cryptographic operations will be as pervasive, cheap and
unremarkable as IP protocol operations have become today. Some things about
this future are already clear. Cryptographic operations will disappear into
the infrastructure. The complexities of cryptography and of cryptographic
key management will be bidden from users. New sorts of protocols will
become practical. New sorts of businesses will be possible. We describe
several such protocols and businesses. Other important aspects of this
future are less clear, such as the social, economic, and political
implications. We hazard guesses at these and other impacts of cryptography
everywhere.  (0 Refs)
  Subfile: B C
  Descriptors: cryptography; politics; protocols; socio-economic effects
  Identifiers: cryptography; IACR; key management; protocols;
socio-economic implications; political implications
  Class Codes: B6120D (Cryptography); B6150M (Protocols); C6130S (Data
security); C5640  (Protocols); C0230  (Economic, social and political
aspects of computing)
  Copyright 2001, IEE


  2/5/2     (Item 1 from file: 144)
DIALOG(R)File 144:Pascal
(c) 2003 INIST/CNRS. All rts. reserv.

  14917350   PASCAL No.: 01-0067294
```

Cryptography everywhere
Advances in cryptology - ASIACRYPT 2000 : Kyoto, 3-7 December 2000

BERSON Thomas A
OKAMOTO Tatsuaki, ed
Anagram Laboratories, P.O. Box 791, Palo Alto, CA 94302, United States; Xerox Palo Alto Research Center, 3333 Coyote Hill Rd, Palo Alto, CA 94304, United States

International conference on the theory and application of cryptology and inforamtion security, 6 (Kyoto JPN) 2000-12-03
Journal: Lecture notes in computer science, 2000, 1976 p. 72
ISBN: 3-540-41404-5 ISSN: 0302-9743 Availability: INIST-16343; 354000092016260060
Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)
Country of Publication: Germany
Language: English

The past twenty years have seen cryptography move from arcane to commonplace, from difficult to easy, from expensive to cheap. Many influences are at work. These include: the professionalization of cryptographers, in which the IACR has played a significant role; the creation of textbooks and of courses; the steady growth of computational power delivered by the operation of Moore's Law; the algorithmic advances made by cryptographic researchers and engineers; the rise of e-commerce and wireless infrastructures which have a seemingly endless appetite for cryptographic services; the entry of many young people into the field; and the easing of government export controls. We envisage a near future where cryptographic operations will be as pervasive, cheap and unremarkable as IP protocol operations have become today. Some things about this future are already clear. Cryptographic operations will disappear into the infrastructure. The complexities of cryptography and of cryptographic key management will be hidden from users. New sorts of protocols will become practical. New sorts of businesses will be possible. We will describe several such protocols and businesses. Other important aspects of this future are less clear, such as the social, economic, and political implications. We will hazard guesses at these and other impacts of cryptography everywhere.

English Descriptors: Communication complexity; Transmission protocol;
Information protection; Cryptography; Computer security

French Descriptors: Complexite communication; Protocole transmission;
Protection information; Cryptographie; Securite informatique

Classification Codes: 001D04A04E

?

```
Set     Items    Description
S1        120    (ENCRYPTION OR CRYPTOGRAPHIC)()SERVICE?
S2    2461554    PRICE OR PRICING OR COST? OR CHARG? OR AMOUNT OR QUOTATION
S3       8680    (COMPUTATION? OR CALCULATION? OR FIGURING OR RECKONING)(2N-
             )(BURDEN? OR CHARGE? OR COMMITMENT? OR DUTY OR OBLIGATION OR -
             RESPONSIBILITY)
S4        262    (PRIVACY OR CONFIDENTIALITY)(2N)(LEVEL OR STATUS OR STANDI-
             NG OR IMPORTANT? OR SCORE? OR RANK?)
S5    5587182    SPEED OR TIME OR TIMING OR PERIOD? OR INTERVAL OR CLOCK OR
             SPACING OR FREQUENCY OR DURATION
S6          9    S1 AND S2
S7          0    S1 AND S3
S8          0    S1 AND S4
S9         23    S1 AND S5
S10         3    S6 AND S9
S11        29    S6 OR S9 OR S10
S12        25    S11 NOT PY>2000
S13        25    S12 NOT PD>20000619
S14        22    RD (unique items)
File   8:Ei Compendex(R) 1970-2003/Dec W2
         (c) 2003 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2003/Nov
         (c) 2003 ProQuest Info&Learning
File 202:Info. Sci. & Tech. Abs. 1966-2003/Nov 17
         (c) 2003 EBSCO Publishing
File  65:Inside Conferences 1993-2003/Dec W3
         (c) 2003 BLDSC all rts. reserv.
File   2:INSPEC 1969-2003/Dec W1
         (c) 2003 Institution of Electrical Engineers
File 233:Internet & Personal Comp. Abs. 1981-2003/Jul
         (c) 2003, EBSCO Pub.
File  94:JICST-EPlus 1985-2003/Dec W3
         (c)2003 Japan Science and Tech Corp(JST)
File  99:Wilson Appl. Sci & Tech Abs 1983-2003/Nov
         (c) 2003 The HW Wilson Co.
File  95:TEME-Technology & Management 1989-2003/Nov W5
         (c) 2003 FIZ TECHNIK
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
?
```

T S14/5/1-5,7-8,10-12,14-16,19-22

14/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

05549572 E.I. No: EIP00055162174
Title: S/390 parallel enterprise server CMOS cryptographic coprocessor
Author: Easter, R.J.; Chencinski, E.W.; D'Avignon, E.J.; Greenspan, S.R.; Merz, W.A.; Norberg, C.D.
Corporate Source: IBM System, Poughkeepsie, NY, USA
Source: IBM Journal of Research and Development v 43 n 5 1999. p 761-776
Publication Year: 1999
CODEN: IBMJAE ISSN: 0018-8646
Language: English
Document Type: JA; (Journal Article) Treatment: G; (General Review)
Journal Announcement: 0006W4

Abstract: As the Internet becomes the basis for electronic commerce, and as more businesses automate their data processing operations, the potential for unauthorized disclosure of sensitive data increases. On-line databases are becoming increasingly large and complex. Sensitive data is transmitted on communication lines and often stored off-line. As a result, the efficient, economical protection of enterprise-critical information is becoming increasingly important in many diverse application environments. The protection required to conduct commerce on the Internet, provide data confidentiality, and provide user authentication can be achieved only by **cryptographic services** and techniques. The high- **speed** , physically secure IBM S/390 CMOS Cryptographic Coprocessor for S/390 Parallel Enterprise Servers, together with the IBM Integrated **Cryptographic Service** Facility (ICSF), an IBM licensed program for the OS/390 operating system, provides the ability to encrypt and decrypt data, generate and manage cryptographic keys, perform PIN operations, and perform other cryptographic functions dealing with data integrity, digital signatures, and key exchange. (Author abstract) 16 Refs.

Descriptors: *Client server computer systems; Internet; Electronic commerce; Database systems; Cryptography; Parallel processing systems; CMOS integrated circuits; Computer hardware
Identifiers: Parallel enterprise server; Cryptographic coprocessor
Classification Codes:
722.4 (Digital Computers & Systems); 723.5 (Computer Applications); 723.3 (Database Systems); 714.2 (Semiconductor Devices & Integrated Circuits)
722 (Computer Hardware); 723 (Computer Software); 714 (Electronic Components)
72 (COMPUTERS & DATA PROCESSING); 71 (ELECTRONICS & COMMUNICATIONS)

14/5/2 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

05520850 E.I. No: EIP00045108892
Title: High Security Modules - still needed despite advances in platforms
Author: Stone, Tim D.; Miller, David
Corporate Source: Baltimore Technologies plc, USA
Source: Information Security Technical Report v 5 n 1 2000. p 42-47
Publication Year: 2000
CODEN: ISTRFR ISSN: 1363-4127
Language: English
Document Type: JA; (Journal Article) Treatment: G; (General Review)

```
  Journal Announcement: 0005W4
  Abstract: High or Host Security Modules (HSM) provide additional
cryptographic security for messages and files. Advances in host processing
capability and the advent of single chip crypto-processors have done little
to dent the need for HSMs. HSMs provide security processing as a service to
a host, usually on request, network security devices generally operate
within the network and provide in-line security to traffic sent over the
network. While each approach has value, the high security devices used to
provide cryptographic   services to hosts are presented. 6 Refs.
  Descriptors: Security of data; Computer systems programming; Response
 time (computer systems); Cryptography; Data communication systems;
Electronic commerce
  Identifiers: High security modules (HSM)
  Classification Codes:
  723.2  (Data Processing); 723.1  (Computer Programming); 722.4  (Digital
Computers & Systems); 723.5  (Computer Applications)
  723  (Computer Software); 722  (Computer Hardware)
  72  (COMPUTERS & DATA PROCESSING)


  14/5/3     (Item 3 from file: 8)
DIALOG(R)File   8:Ei Compendex(R)
(c) 2003 Elsevier Eng.  Info. Inc. All rts. reserv.

05193238   E.I. No: EIP98124513088
 Title: Inline network encryption for multimedia wireless LANs
  Author: Ganz, Aura; Park, Se Hyun; Ganz, Zvi
  Corporate Source: Univ of Massachusetts, Amherst, MA, USA
  Conference  Title:  Proceedings  of the 1998 IEEE Military Communications
Conference. Part 2 (of 3)
  Conference     Location:     Bedford,    MA,    USA   Conference    Date:
19981019-19981021
  Sponsor: IEEE
  E.I. Conference No.: 49416
  Source:  Proceedings - IEEE Military Communications Conference MILCOM v 2
1998. IEEE, Piscataway, NJ, USA,98CH36201. p 560-564
  Publication Year: 1998
  CODEN: PMICET
  Language: English
  Document Type: CA; (Conference Article)   Treatment: G; (General Review)
  Journal Announcement: 9902W3
  Abstract: To secure real- time communication in wireless LANs it is
pertinent to implement real time   cryptographic   services in software
or hardware. In this paper we evaluate the use of software based inline
encryption algorithms for wireless LANs that are implemented in the Layer
Service Provider as defined by WinSock 2 for Windows. The evaluated
encryption algorithms run on each PC that is part of the wireless LAN. We
present the throughput requirements from the inline encryptors for various
multimedia applications such as video conferencing, collaborative work,
distributed data bases and distributed processing. Our measurements show
that software implementation of various encryptors provides enough
throughput as required by the above applications. (Author abstract) 11
Refs.
  Descriptors: Local area networks; Wireless telecommunication systems;
Multimedia systems; Cryptography; Security of data; Real time systems;
Telecommunication services; Groupware; Computer hardware; Algorithms
  Identifiers: Inline network encryption
  Classification Codes:
  723.5  (Computer Applications); 723.2  (Data Processing); 722.4  (Digital
Computers & Systems)
```

716 (Radar, Radio & TV Electronic Equipment); 723 (Computer Software);
722 (Computer Hardware)
71 (ELECTRONICS & COMMUNICATIONS); 72 (COMPUTERS & DATA PROCESSING)

14/5/4 (Item 4 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)
(c) 2003 Elsevier Eng. Info. Inc. All rts. reserv.

02160736 E.I. Monthly No: EI8701002499
Title: SBS LAUNCHES PUBLIC SWITCHED ENCRYPTION SERVICE□.□
Author: Anon
Source: Electronics v 59 n 6 Feb 10 1986 p 38-40
Publication Year: 1986
CODEN: ELECEH
Language: ENGLISH
Document Type: JA; (Journal Article) Treatment: A; (Applications)
Journal Announcement: 8701

Abstract: Encryption, long favored by the military to protect its traffic, is already protecting the networks of large corporations. But it is **costly** to implement and has not been generally available in public switched networks. Means to secure the telecommunications traffic on a common-carrier subnetwork at **costs** competitive with nonencrypted services are introduced by Satellite Business Systems (SBS) that treats large amounts of traffic in bulk through a single encryption unit before it enters the satellite transmission system. Only one bulk-encryption unit per earth station is required on the SBS network. The encryption unit meets rigid federal standards for physical security and implements a variation of the government's Data Encryption Standard (DES) output-feedback mode using two keys - a master and a working key. The master key is used to decrypt a working key that is changed **periodically** .

Descriptors: *CRYPTOGRAPHY; TELECOMMUNICATION LINKS, SATELLITE--Protection; DIGITAL COMMUNICATION SYSTEMS--Voice/Data Integrated Services; DATA PROCESSING--Security of Data

Identifiers: PUBLIC SWITCHED ENCRYPTION; DATA ENCRYPTION STANDARD (DES); MASTER KEY; WORKING KEY

Classification Codes:
723 (Computer Software); 716 (Radar, Radio & TV Electronic Equipment);
718 (Telephone & Line Communications)
72 (COMPUTERS & DATA PROCESSING); 71 (ELECTRONICS & COMMUNICATIONS)

14/5/5 (Item 5 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)
(c) 2003 Elsevier Eng. Info. Inc. All rts. reserv.

01913518 E.I. Monthly No: EIM8512-079801
Title: PROJECT UNIVERSE ENCRYPTION EXPERIMENT.
Author: Jackson, A. M.; McEvoy, N. A.; Newman, B. B.
Corporate Source: GEC Research Lab, Marconi Research Cent, UK
Conference Title: International Conference on Secure Communication Systems.
Conference Location: London, Engl Conference Date: 19840222
Sponsor: IEE, Electronics Div, London, Engl; IEE, Computing & Control Div, London, Engl; British Computer Soc, London, Engl; Inst of Acoustics, Edinburgh, Scotl; Inst of Physics, London, Engl
E.I. Conference No.: 05466
Source: IEE Conference Publication n 231. Publ by IEE, London, Engl p 14-19
Publication Year: 1984

CODEN: IECPB4 ISBN: 0-85296288-6
Language: English
Document Type: PA; (Conference Paper)
Journal Announcement: 8512

Abstract: Project UNIVERSE is a major experiment in high bandwidth Wide Area Networks undertaken by a consortium of industrial and academic institutions. Those involved are British Telecom, Cambridge University, the Department of Trade and Industry, GEC Research Laboratories-Marconi Research Centre (MRC), Logica Ltd. , Loughborough University of Technology, the Science and Engineering Research Council and University College London. Local Area Networks at seven sites are connected via a communications satellite and high- **speed** terrestrial links. The risk of interception is particularly acute in a satellite network because of the broadcast nature of the downlink. Therefore, as part of Project UNIVERSE, Logica and MRC have designed and implemented an encryption system to enable secure end-to-end communication across the UNIVERSE network. The system is based on the United States Data Encryption Standard (DES) which Logica has implemented in software and MRC in hardware. An 'encryption layer protocol' has been developed which enables any application to use the **encryption service** in a transparent fashion. 7 refs.

Descriptors: *TELECOMMUNICATION SYSTEMS, SATELLITE RELAY--*Protection; TELECOMMUNICATION LINKS, SATELLITE; COMPUTER NETWORKS--Local Networks; CRYPTOGRAPHY--Applications

Identifiers: WIDE AREA NETWORKS; LOCAL AREA NETWORKS; NETWORK TOPOLOGY; DATA ENCRYPTION STANDARD (DES); PUBLIC KEY CRYPTOGRAPHY (PKC)

Classification Codes:
716 (Radar, Radio & TV Electronic Equipment); 717 (Electro-Optical Communications); 718 (Telephone & Line Communications); 655 (Spacecraft); 723 (Computer Software)
71 (ELECTRONICS & COMMUNICATIONS); 65 (AEROSPACE ENGINEERING); 72 (COMPUTERS & DATA PROCESSING)

14/5/7 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2003 Institution of Electrical Engineers. All rts. reserv.

6435010 INSPEC Abstract Number: B2000-01-6210L-146, C2000-01-5620L-058

Title: Experimental measurements and design guidelines for real- time **software encryption in multimedia wireless LANs**
Author(s): Ganz, A.; Se Hyun Park; Ganz, Z.
Author Affiliation: Dept. of Electr. & Comput. Eng., Massachusetts Univ., Amherst, MA, USA
Journal: Cluster Computing vol.2, no.1 p.35-43
Publisher: Baltzer,
Publication Date: 1999 Country of Publication: Netherlands
CODEN: CLCOFM ISSN: 1386-7857
SICI: 1386-7857(1999)2:1L.35:EMDG;1-U
Material Identity Number: H401-1999-004
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P)

Abstract: To secure interactive multimedia applications in wireless LANs (WLANs), it is pertinent to implement real **time cryptographic services** . We evaluate the use of software based encryption algorithms that are implemented in the layer service provider as defined by WinSock 2 for Windows 95/NT. Our measurements show that software implementation of various encryptors can sustain the throughput requirements of interactive multimedia applications for WLANs such as telephone quality audio, video conferencing, and MPEG video. We present a design methodology that includes guidelines for a secure multimedia system design in terms of the encryption method chosen as a function of required application throughput, system configuration, protocol layers overhead and wireless LAN throughput. (12 Refs)

Subfile: B C

Descriptors: cryptography; interactive systems; multimedia communication; real- **time** systems; wireless LAN

Identifiers: experimental measurements; design guidelines; real **time** software encryption; multimedia wireless LANs; secure interactive multimedia applications; WLANs; real **time cryptographic services** ; software based encryption algorithms; layer service provider; WinSock 2; software implementation; encryptors; throughput requirements; interactive multimedia applications; telephone quality audio; video conferencing; MPEG video; design methodology; secure multimedia system design; encryption method; application throughput; system configuration; protocol layers overhead; wireless LAN throughput

Class Codes: B6210L (Computer communications); B6210R (Multimedia communications); B6250 (Radio links and equipment); B6120D (Cryptography); C5620L (Local area networks); C6130M (Multimedia); C6130S (Data security); C6180 (User interfaces)

Copyright 1999, IEE

14/5/8 (Item 3 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2003 Institution of Electrical Engineers. All rts. reserv.

6258886 INSPEC Abstract Number: B1999-07-6210L-041, C1999-07-5620L-016

Title: Inline network encryption for multimedia wireless LANs

Author(s): Aura Ganz; Se Hyun Park; Ganz, Z.

Author Affiliation: Multimedia Wireless LAN Lab., Massachusetts Univ., Amherst, MA, USA

Conference Title: IEEE Military Communications Conference. Proceedings. MILCOM 98 (Cat. No.98CH36201) Part vol.2 p.560-4 vol.2

Publisher: IEEE, New York, NY, USA

Publication Date: 1998 Country of Publication: USA 3 vol. xxxv+1083 pp.

ISBN: 0 7803 4506 1 Material Identity Number: XX-1998-03092

U.S. Copyright Clearance Center Code: 0 7803 4506 1/98/$10.00

Conference Title: IEEE Military Communications Conference. Proceedings. MILCOM 98

Conference Date: 18-21 Oct. 1998 Conference Location: Boston, MA, USA

Language: English Document Type: Conference Paper (PA)

Treatment: Applications (A); Practical (P); Experimental (X)

Abstract: To secure real- **time** communication in wireless LANs it is pertinent to implement real **time cryptographic services** in software or hardware. We evaluate the use of software based inline encryption algorithms for wireless LANs that are implemented in the Layer Service Provider as defined by WinSock 2 for Windows. The evaluated encryption algorithms run on each PC that is part of the wireless LAN. We present the throughput requirements from the inline encryptors for various multimedia applications such as video conferencing, collaborative work, distributed data bases and distributed processing. Our measurements show that software implementation of various encryptors provides enough throughput as required by the above applications. (11 Refs)

Subfile: B C

Descriptors: cryptography; distributed databases; groupware; microcomputer applications; multimedia communication; telecommunication security; teleconferencing; wireless LAN

Identifiers: multimedia wireless LAN; inline network encryption; secure real- **time** communication; real **time cryptographic services** ; hardware

; inline encryption algorithms; Layer Service Provider; WinSock 2 for Windows; PC; personal computer; throughput; video conferencing; collaborative work; distributed data bases; distributed processing; measurements; software implementation

Class Codes: B6210L (Computer communications); B6250 (Radio links and equipment); B6210R (Multimedia communications); B6120D (Cryptography); C5620L (Local area networks); C6130M (Multimedia); C6130S (Data security); C6130G (Groupware); C6150N (Distributed systems software)

Copyright 1999, IEE

14/5/10 (Item 5 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2003 Institution of Electrical Engineers. All rts. reserv.

5865749 INSPEC Abstract Number: B9805-6210C-005, C9805-7100-001

Title: Extranet security: what's right for the business?

Author(s): Trolan, S.

Author Affiliation: Altera Corp., San Jose, CA, USA

Journal: Information Systems Security vol.7, no.1 p.47-56

Publisher: Auerbach Publications,

Publication Date: Spring 1998 Country of Publication: USA

CODEN: ISSEFH ISSN: 1065-898X

SICI: 1065-898X(199821)7:1L.47:ESWR;1-I

Material Identity Number: F173-98002

Language: English Document Type: Journal Paper (JP)

Treatment: Practical (P)

Abstract: Extranets are the evolution of business requirements to create a separate and distinct category of network participants; for lack of a more descriptive phrase, that is neither intranet nor Internet. By the year 2000, estimates are that computer access will come from external associations. This rise in external access is coming from telecommuters, business associates, customers, or potential customers, each with a unique set of computing and data requirements. The solution will not be the same for all-more aptly stated, it should not be the same for all. Choosing the best extranet solution for a company's needs is important. To choose the correct solution, it is important to understand clearly the available alternatives. There are six basic extranet technologies as well as some specialized and hybrid solutions: (1) external resources; (2) Internet protocol (IP) address filtering; (3) authentication servers; (4) application layer management; (5) proxy servers; and (6) **encryption services** . Each is sufficient to initiate business communications, but each carries different performance, **cost** , and security. A detailed review of each technology is presented. (0 Refs)

Subfile: B C

Descriptors: business communication; business data processing; computer network management; network servers; security of data

Identifiers: extranet security; business requirements; network participants; computer access; external associations; telecommuters; business associates; potential customers; data requirements; extranet solution; extranet technologies; external resources; Internet protocol address filtering; authentication servers; application layer management; proxy servers; **encryption services** ; business communications

Class Codes: B6210C (Network management); B6210L (Computer communications); C7100 (Business and administration); C0310D (Computer installation management); C5620 (Computer networks and techniques); C6130S (Data security); C0230 (Economic, social and political aspects of computing)

Copyright 1998, IEE

14/5/11 (Item 6 from file: 2)
DIALOG(R)File 2:INSPEC

5755308 INSPEC Abstract Number: C9801-6130E-001
Title: The United Kingdom policy on trusted third parties and its implications for EDI
Author(s): Reed, C.; Avellan, J.
Author Affiliation: Inf. Technol. Law Unit, Queen Mary & Westfield Coll., London, UK
Journal: EDI Law Review vol.4, no.2 p.81-9
Publisher: Kluwer Law International,
Publication Date: 1997 Country of Publication: Netherlands
CODEN: EDLRE7 ISSN: 0929-2233
SICI: 0929-2233(1997)4:2L.81:UKPT;1-O
Material Identity Number: D356-97005
U.S. Copyright Clearance Center Code: 0929-2233/97/$9.50
Language: English Document Type: Journal Paper (JP)
Treatment: General, Review (G)

Abstract: As part of the British government's efforts to keep pace with the changes produced by the established and emerging network technologies and their corresponding by-products, such as the widespread use of cryptography, in June 1996 a report was published by the Department of Trade and Industry (DTI) entitled "Paper on Regulatory Intent Concerning Use of Encryption on Public Networks". This report was followed in March 1997 with a public consultation paper on detailed proposals for legislation, "Licensing of Trusted Third Parties for the Provision of **Encryption Services** ". During the public consultation **period** , which ended 30 May, 1997, public comments were requested on the contents of the legislative proposal and a meeting was held allowing the general public to voice their opinions. The public comments have been analysed and they will be presented to the new government so that it may determine whether legislation will be passed and the scope of such legislation. This article presents some of the implications the published policy could have for the use, offer and/or provision of EDI communications. (15 Refs)

Subfile: C
Descriptors: cryptography; electronic data interchange; government policies; legislation
Identifiers: United Kingdom policy; trusted third parties; EDI; British government; network technologies; cryptography; Department of Trade and Industry; legislation; electronic data interchange
Class Codes: C6130E (Data interchange); C0230 (Economic, social and political aspects of computing); C6130S (Data security)
Copyright 1997, IEE

14/5/12 (Item 7 from file: 2)
DIALOG(R)File 2:INSPEC

5575625 INSPEC Abstract Number: C9706-0230B-010
Title: Trusted third parties and the provision of encryption services
Author(s): Hill, J.
Journal: Computers and Law vol.8, no.1 p.30-3
Publisher: Soc. Comput. & Law,
Publication Date: April-May 1997 Country of Publication: UK
CODEN: CLAWDY ISSN: 0140-3249
SICI: 0140-3249(199704/05)8:1L.30:TTPP;1-3
Material Identity Number: M548-97003
Language: English Document Type: Journal Paper (JP)

Treatment: General, Review (G)
Abstract: Trusted third party (TTP) is defined as an entity trusted by other entities with respect to security related services and activities and **encryption services** as encompassing any service, whether provided free or not, which involves any or all of the following cryptographic functionality-key management, key recovery, key certification, key storage, message integrity (through the use of digital signatures), key generation, **time** stamping, or key revocation services (whether for integrity or confidentiality), which are offered in a manner which allows a client to determine a choice of cryptographic key or allows the client a choice of recipient. The paper raises too many issues to be dealt with fully; the article attempts only to highlight a few of the most obvious ones, and to try to clarify where possible those that relate to TTPs operating as certification authorities and those as key escrow/key recovery agencies. (0 Refs)
Subfile: C
Descriptors: certification; cryptography; Internet; legislation
Identifiers: **encryption services** ; trusted third parties; security related services; security related activities; cryptographic functionality; key management; key recovery; key certification; key storage; message integrity; key generation; **time** stamping; key revocation services; cryptographic key; certification authorities; key escrow agencies; key recovery agencies
Class Codes: C0230B (Legal aspects of computing); C6130S (Data security)
Copyright 1997, IEE

14/5/14 (Item 9 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2003 Institution of Electrical Engineers. All rts. reserv.

02824834 INSPEC Abstract Number: B87012925, C87011885
Title: Implementation of an encrypted open system local area network
Author(s): Dowler, B.R.
Author Affiliation: Div. of Network Syst., IBM, London, UK
Conference Title: Second International Conference on Secure Communication Systems (Conf. Publ. No.269) p.39-42
Publisher: IEE, London, UK
Publication Date: 1986 Country of Publication: UK 130 pp.
ISBN: 0 85296 339 4
Conference Sponsor: IEE
Conference Date: 27-28 Oct. 1986 Conference Location: London, UK
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: Shows the practicality of providing security via encryption without significant performance degradation for Open Systems Networks by producing and demonstrating an encrypting relay unit that is situated between an end system and the network. The author also produces a unique proprietary encryption algorithm implemented in a custom VLSI device for use within an **encryption service** . Although this phase of development has been concluded, work is still continuing on the integration of the **encryption service** directly into the end-system, whether mainframe, server, or workstation, with the ultimate intention of providing encryption as a standard facility available easily and at low **cost** . (2 Refs)
Subfile: B C
Descriptors: cryptography; local area networks
Identifiers: encrypted open system local area network; security; encryption; custom VLSI device; standard facility
Class Codes: B6120B (Codes); B6210L (Computer communications); C5620L (Local area networks); C6130 (Data handling techniques)

14/5/15 (Item 1 from file: 233)

DIALOG(R)File 233:Internet & Personal Comp. Abs.
(c) 2003, EBSCO Pub. All rts. reserv.

00522234 99EA01-006

X12 EDI security: safe passage over the Internet -- X12 standards exemplify the security functionality needed across the EDI spectrum as companies transition to Web-based EDI

DeGrafft, Hart W
e-Business Advisor , January 1, 1999 , v17 n1 p36-39, 4 Page(s)
ISSN: 1098-8912
Languages: English
Document Type: Articles, News & Columns
Geographic Location: United States

Traces the evolution of the Electronic Data Interchange (EDI) X12 standards, explains security services established by the standards, and mentions the need to extend the EDI security standards to increasingly available Web-based EDI in business. Mentions the X12 EDI standards began addressing security in the 1980s through the needs of the financial business community. Details the two main security services: electronic digital signature, and data encryption. Explains the X12.58 Security Structures Standard and the X12.815 **Cryptographic Service** Message Standard. Explains the way data compression offsets the added overhead and **cost** . Explains important ways that X12.58 and X12.815 complement each other. Mentions that X12.58 provides network/protocol independence by serving end-to-end protection. Says the existing standards have potential to be extended to the Web environment. Includes one sidebar. (bjp)

Descriptors: Electronic Data Interchange; Standards; Security; Business; Definitions

14/5/16 (Item 2 from file: 233)

DIALOG(R)File 233:Internet & Personal Comp. Abs.
(c) 2003, EBSCO Pub. All rts. reserv.

00510188 98SR10-003

IW Folder -- This product brings encryption services **to the desktop in as clean and easy a manner as we can imagine**

SC/INFO SECURITY NEWS MAGAZINE , October 1, 1998 , v9 n10 p28, 1 Page(s)
ISSN: 1096-7974
Company Name: SunBurst Technologies
URL: http://www.aec-security.com
Product Name: IW Folder
Languages: English
Document Type: Software Review
Grade (of Product Reviewed): B
Hardware/Software Compatibility: IBM PC Compatible; Microsoft Windows; Microsoft Windows 95; Microsoft Windows NT
Geographic Location: United States

Presents a favorable review of IW Folder ($25), a security program from SunBurst Technology Inc. (503). Says that this program is a useful tool for assuring confidentiality of data on a machine in an open office or on shared PCs. Explains that the package offers a management tool for editing which subdirectory is associated with a user/password. Adds that more than one subdirectory may be specified in this case. However, says that decryption occurs only at system start-up **time** and re-encryption occurs only during an orderly end process, meaning that if there is a power failure, then the files are available to anyone who wants to look for them.

Adds that bundled with IW Folder is IW Bin, a secure deletion process that deletes the name of a file and overwrites every used byte so that it cannot be retrieved. Concludes IW Folder is extremely easy to operate but notes the documentation could have been more useful. Contains one photo. (EB)

Descriptors: Security; Encryption; File Management
Identifiers: IW Folder; SunBurst Technologies

14/5/19 (Item 1 from file: 583)

DIALOG(R)File 583:Gale Group Globalbase(TM)
(c) 2002 The Gale Group. All rts. reserv.

09070069
Moves to build trust in Internet trading
UK: GOVERNMENT PUBLISHES E-COMMERCE PAPER
Independent (TI) 06 Mar 1999 p.19
Language: ENGLISH

The UK Government has published a consultation paper on electronic commerce as a preliminary to legislation which the Government hopes will make the UK the best setting for e-commerce trading in the world by 2002. It is vital the UK does not get left behind as the way we do business is set to change dramatically in the near future and there is a need to keep up. With this legislation the Government hopes to improve public trust in trading via the Internet and at the same **time** remove legal barriers regarding electronic signatures which have held back the progress of e-commerce in the UK. Of major concern is security when making purchases online. The paper is looking for views on several major issues including; updating the law so contracts can be signed electronically; setting up a voluntary licensing system for business which are prepared to provide the **encryption service** . A task force has been established to gather opinions on such matters, and all responses should be made by April 01 1999.

EVENT: Government Regulations (93);
COUNTRY: United Kingdom (4UK);

14/5/20 (Item 2 from file: 583)

DIALOG(R)File 583:Gale Group Globalbase(TM)
(c) 2002 The Gale Group. All rts. reserv.

06605939
Bezeq trials low **cost encryption service**
ISRAEL: BEZEQ'S LOW **COST** ENCRYPTION LAUNCHED
CommunicationsWeek International (CWI) 2 Mar 1998 p.10
Language: ENGLISH

Israeli telecoms firm, Bezeq, are responding to the demand for secure telephone lines among business users by launching a test for a low- **cost encryption service** . Bezeq hopes to have the service available by early 1999 at the latest. The company believes that the demand for such a product is high, putting this down to media reports of cellular telephones being tapped and other illegal wiretapping. A Bezeq survey said that 25% of business users would be interested in a form of telephone security.

COMPANY: BEZEQ

PRODUCT: Telephone Communications (4811); Telecommunications (4810);
Computer & Data Security Software (7372CD);
EVENT: Product Design & Development (33); Product Standards (35);
National Government Economics (94);

COUNTRY: Israel (8ISR);

14/5/21 (Item 3 from file: 583)
DIALOG(R)File 583:Gale Group Globalbase(TM)

06104648
Next Generation Digital Cellular Phone Call
US: ADVANCE IN CELLULAR DIGITAL PHONE SERVICES
Telecommunications News (ZCD) 15 Jan 1995 p.3
Language: ENGLISH

New Digital Technology for **Time** Division Multiple Access (TDMA) has been used by three telephone firms - <US> firm McCaw Cellular, <Finnish> firm Nokia Mobile Phones and <Swedish> firm Ericsson - to make the first ever cellular digital phone call. The latest type of TDMA used, IS-136, has officially been declared as the next cellular digital network level by the Telecommunications Industry Association. The infrastructure for this telephone first was made by Ericsson. The IS-136 technology allows caller line identification and **encryption services** as well as giving greater line capacity.

COMPANY: TELECOMMUNICATIONS INDUSTRY ASSN; ERICSSON; NOKIA MOBILE PHONES; MCCAW CELLULAR

PRODUCT: Cellular Radio Services (4811CR);
EVENT: Product Design & Development (33);
COUNTRY: Sweden (5SWE); Finland (5FIN); United States (1USA);

14/5/22 (Item 4 from file: 583)
DIALOG(R)File 583:Gale Group Globalbase(TM)

01862495
TELENET LAUNCHES X.25 **ENCRYPTION SERVICE**
US - TELENET LAUNCHES X.25 **ENCRYPTION SERVICE**
Telephony (TLY) 4 April 1988 p18
ISSN: 0040-2656

Telenet Communications has launched an X.25 packet-data network **encryption service** . The new service will give end-to-end security for synchronous, asyschronous, dial-up and dedicated network customers. The X.25 **encryption service** will be linked to Telenet's Access Management System, providing greater security for its 2000 host computers. The **encryption service** will have an additional **cost** of USD1r200 per access point on top of **charges** for TAMS.

PRODUCT: Data Communications Equipment (3661DC); Data Communications (4811DC); Private Telephone Systems (4811PE);
EVENT: PRODUCTS, PROCESSES & SERVICES (30);
COUNTRY: United States (1USA); NATO Countries (420); South East Asia Treaty Organisation (913);
?

```
Set     Items   Description
S1       1590   (ENCRYPTION OR CRYPTOGRAPHIC)()SERVICE?
S2    9328444   PRICE OR PRICING OR COST? OR CHARG? OR AMOUNT OR QUOTATION
S3       1752   (COMPUTATION? OR CALCULATION? OR FIGURING OR RECKONING)(2N-
             )(BURDEN? OR CHARGE? OR COMMITMENT? OR DUTY OR OBLIGATION OR -
             RESPONSIBILITY)
S4       3689   (PRIVACY OR CONFIDENTIALITY)(2N)(LEVEL OR STATUS OR STANDI-
             NG OR IMPORTANT? OR SCORE? OR RANK?)
S5    8741749   SPEED OR TIME OR TIMING OR PERIOD? OR INTERVAL OR CLOCK OR
             SPACING OR FREQUENCY OR DURATION
S6        162   S1 (S) S2
S7          0   S6 (S) S3
S8          0   S6 (S) S4
S9         40   S6 (S) S5
S10        29   S9 NOT PY>2000
S11        24   S10 NOT PD>20000619
S12        21   RD (unique items)
File  15:ABI/Inform(R) 1971-2003/Dec 20
         (c) 2003 ProQuest Info&Learning
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 647:CMP  Computer Fulltext 1988-2003/Dec W3
         (c) 2003 CMP Media, LLC
File 275:Gale Group Computer DB(TM) 1983-2003/Dec 23
         (c) 2003 The Gale Group
File 674:Computer News Fulltext 1989-2003/Dec W1
         (c) 2003 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2003/Dec 22
         (c) 2003 The Dialog Corp.
File 624:McGraw-Hill Publications 1985-2003/Dec 22
         (c) 2003 McGraw-Hill Co. Inc
File 636:Gale Group Newsletter DB(TM) 1987-2003/Dec 23
         (c) 2003 The Gale Group
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 613:PR Newswire 1999-2003/Dec 23
         (c) 2003 PR Newswire Association Inc
File  16:Gale Group PROMT(R) 1990-2003/Dec 23
         (c) 2003 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 553:Wilson Bus. Abs. FullText 1982-2003/Nov
         (c) 2003 The HW Wilson Co
?
```

```
T S12/5,K/ALL

  12/5,K/1     (Item 1 from file: 15)
DIALOG(R)File  15:ABI/Inform(R)
(c) 2003 ProQuest Info&Learning. All rts. reserv.

01776592  04-27583
                     **USE FORMAT 9 FOR FULL TEXT**
 Developments in the use of encryption
Corbitt, Terry
Management  Accounting-London  v77n1  PP: 62  Jan 1999 CODEN: MATGBA  ISSN:
    0025-1682  JRNL CODE: MAC
DOC TYPE: Journal article  LANGUAGE: English   LENGTH: 1 Pages
WORD COUNT: 1250

ABSTRACT:  With the increasing growth of the internet and the desire of the
business world to use it for electronic commerce, encryption is a necessity
for  security.  The government is preparing to regulate electronic commerce
and  legislation  is  expected for this in 1999. There are 4 requisites for
trusted communication: 1. authentication, 2. non-repudiation, 3. integrity,
4.  encryption.  To  implement  a  framework  for  electronic  commerce the
government  proposes  legislation on encryption giving legal recognition to
digital  signatures  for the first time. It will also implement a voluntary
licensing scheme for CAs or other providers of encryption services.

GEOGRAPHIC NAMES: UK
DESCRIPTORS: Data encryption; Data integrity; Computer security;
   Legislation; Electronic commerce
CLASSIFICATION CODES: 9175 (CN=Western Europe); 5140 (CN=Security); 5250
   (CN=Telecommunications systems); 4320 (CN=Legislation)

...TEXT:  electronic  commerce  the  government  proposes  legislation  on
encryption  giving  legal  recognition  to digital signatures for the first
  time  .  It  will  also implement a voluntary licensing scheme for CAs or
other  providers  of  encryption   services  . Licensed organisations would
have  to deposit copies of scrambling keys with bodies called Trusted Third
Parties (TTPs...

... by  police  and  security  agencies.  Privacy  advocates,  human rights
activists  and  software  vendors  oppose keyescrow as a costly mechanism
that  threatens  civil  liberties.  Phillip  Zimmermann, the creator of the
encryption program called Pretty Good Privacy...


 12/5,K/2     (Item 1 from file: 647)
DIALOG(R)File 647:CMP  Computer Fulltext
(c) 2003 CMP Media, LLC. All rts. reserv.

00515282   CMP ACCESSION NUMBER: IWK19920810S1984
 WEAK LINKS - For corporate spies, low-tech communications  are easy marks
Mary E. Thyfault and Stephanie Stahl with Joseph C. Panettieri
INFORMATIONWEEK, 1992, n 386, 26
PUBLICATION DATE: 920810
JOURNAL CODE: IWK     LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: COVER STORY
WORD COUNT: 2313
TEXT:
     Don't look now, but somebody may be watching you.
```

... Ratliffe. But that doesn't seem to concern most users. Although Kirkland, Wash.-based McCaw offers an **encryption** **service** that carries a $500 one- **time** hardware **cost** , plus a monthly service□charge□of $15 to $30, "We don't have a lot of takers," says Ratliffe.

"Not many of...

12/5,K/3 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2003 The Gale Group. All rts. reserv.

02281078 SUPPLIER NUMBER: 54211179 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Certificates, keys, and security.(security concerns relating to Internet use)(Internet/Web/Online Service Information)
Pleas, Keith
PC Magazine, 203(1)
April 20, 1999
ISSN: 0888-8507 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 3603 LINE COUNT: 00290

ABSTRACT: Technologies such as digital certificates and public key encryption are taking on increased significance as the Internet rapidly takes on more importance in our corporate and individual lives. Digital certificates are issued by certificate authorities (CA). Certificates, which are signed with private keys and verified with public keys, are used for establishing secure Web connections, authenticating Web clients, encrypting and signing e-mail transmissions, and publishing software.

GEOGRAPHIC CODES/NAMES: 1USA United States
DESCRIPTORS: Internet/Web technology; Encryption; Digital signature; Privacy issue; Public key encryption
FILE SEGMENT: CD File 275
... organization.

Why would an organization want to be a root CA? Often, it's a matter of **cost** . VeriSign's OnSite license, for example, is priced from $4,000 for up to 500 users to...direct user interface, and works with both Microsoft and non-Microsoft browsers and Web servers. It uses **Cryptographic** **Service** Providers (CSPs) and the CryptoAPI under the hood and is accessed through several programmable objects and command...

...a more complete user interface, built-in support for CA hierarchies, and additional capabilities such as a **time** -stamping server.

Digital Certificates

The most common form of digital certificates are signature certificates, which contain some...

12/5,K/4 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2003 The Gale Group. All rts. reserv.

02038456 SUPPLIER NUMBER: 19146503 (USE FORMAT 7 OR 9 FOR FULL TEXT)
OPENVISION PLANS APPLICATION SPECIFIC MANAGEMENT AND BACK-UP TOOLS - THE FIRST STOP IS SAP'S R/3.
Computergram International, n3102, pCGN02180008
Feb 18, 1997
ISSN: 0268-716X LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 282 LINE COUNT: 00025

FILE SEGMENT: CD File 275

TEXT:

...analysis. As well as making R/3 sites more robust, OpenVision says the aim is to reduce **cost** of ownership, claiming that many first- **time** SAP customers overspend on their first purchase by trying to project too far into the future. Research house International Data Corp says the **cost** of ownership of an R/3 system is at least ten times its product **price** . OpenVision developed Axxion for SAP over at Bay Networks Inc, which went overboard on its SAP installation...

...a nightmare trying to put the thing together and manage it. A range of security, authentication and **encryption** **services** can now be plugged into R/3 via the programming interfaces SAP is integrating on OpenVision's ...

...set to start in April, priced from $175,000 for a database and three application servers. The **price** rises as application servers are added. OpenVision plans other custom Axxion suites for the other applications, such...

12/5,K/5 (Item 3 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2003 The Gale Group. All rts. reserv.

01803139 SUPPLIER NUMBER: 17221440
UUNet and Motorola unwrap wares for nonclassified nets.
Sikorovsky, Elizabeth
Federal Computer Week, v9, n12, p28(2)
May 29, 1995
ISSN: 0893-052X LANGUAGE: English RECORD TYPE: Abstract

ABSTRACT: UUNet Technologies and Motorola are both releasing network security suites. The products are targeted at federal users who would like to conduct secure, high- **speed** communications over the Internet. Conducting these communications over the Internet offers a big **price** advantage over use of value-added networks. Products like the ones being released by take away a significant **amount** of traffic from the value-added networks. UUNet currently provides high- **speed** data encryption using the Data Encryption Standard (DES), a firewall, authentication, and security consulting. The services provide a way for users to conduct research and CAD over the Internet, and also permits users to share documents securely in real **time** . The company attempts to create a virtual network over the Internet for its customers. Motorola will also be offering its own firewall and DES **encryption** **services** through a new business unit.

COMPANY NAMES: Motorola Inc.--Services; UUNet Technologies Inc.--Services
DESCRIPTORS: Company Services; Company Service Introduction; Network Security Software; Internet
TICKER SYMBOLS: MOT
FILE SEGMENT: CD File 275

...ABSTRACT: network security suites. The products are targeted at federal users who would like to conduct secure, high- **speed** communications over the Internet. Conducting these communications over the Internet offers a big **price** advantage over use of value-added networks. Products like the ones being released by take away a significant **amount** of traffic from the value-added networks. UUNet currently provides high- **speed** data encryption using the Data Encryption Standard (DES), a firewall, authentication, and security consulting. The services provide...

...conduct research and CAD over the Internet, and also permits users to share documents securely in real **time** . The company attempts to create a virtual network over the Internet for its customers. Motorola will also be offering its own firewall and DES **encryption services** through a new business unit.

12/5,K/6 (Item 1 from file: 674)
DIALOG(R)File 674:Computer News Fulltext
(c) 2003 IDG Communications. All rts. reserv.

080049
Front News
Journal: Network World Page Number: 6
Publication Date: December 13, 1999
Word Count: 666 Line Count: 62

Text:
...a first-day percentage gain on Wall Street. VA Linux, which started the day with an offer **price** of $30, saw its shares rise to a high of $320 before closing at $239.25 on...

...alternative to Microsoft's Windows operating system that has been touted by some as a strong, low- **cost** platform for Web servers.BroadVision broadens visionLast week, e-commerce software provider BroadVision made its first acquisition...

... systems meet the basic Level 1 requirements of the FIPS 140-1 standard. In other words, the **encryption services** work without known flaws.Nice day at the optical beachThere hasn't been much opportunity to get...

... called Qtera, and if a rumored $2.5 billion to $3.5 billion deal goes through, that **time** is running out. Nortel Networks is reported to be sniffing around the year-old Boca Raton start...

...will be ready to ship technology that enables all-optical transport gear that can cut the equipment **cost** for long-haul fiber networks by 90%. The deal would not only enrich Nortel's fiber-optic...

12/5,K/7 (Item 1 from file: 696)
DIALOG(R)File 696:DIALOG Telecom. Newsletters
(c) 2003 The Dialog Corp. All rts. reserv.

00697387
ELECTRONIC COMMERCE
TELECOMS STANDARDS & APPROVALS REVIEW
October 20, 1999 VOL: 4 ISSUE: 9 DOCUMENT TYPE: NEWSLETTER
PUBLISHER: PHILLIPS BUSINESS INFORMATION
LANGUAGE: ENGLISH WORD COUNT: 540 RECORD TYPE: FULLTEXT

Standard for electronic signature Aware that Electronic Commerce is the future way of conducting business between companies across local, wide area and global networks such as the Internet,

(c) PHILLIPS PUBLISHING INTERNATIONAL All Rts. Reserv.

COMPANY NAME(S): American Management Systems Inc ; AMSis Telecommunications Industry Group ; Business Solutions ; Chief ; Confederation of British

Industry ; Electronic Commerce ; ETSI SECURITY

TEXT:
...published a draft ETSI Standard, ES 201 733: "Electronic signature standardisation for business transactions . Following a **period** for public comment the document will go for approval by the ETSI SECURITY project and finally for...

...severe difficulties. Earlier this year the UK government abandoned proposals to enforce a key escrow procedure for **encryption services** . But the current draft of the Electronic Communications Bill is the subject of much criticism from the...intercept electronic transactions and gain access to confidential data. The concerns expressed are about the practicality and **cost** of providing for this access; not the principle of giving such powers to the government agencies. There...

12/5,K/8 (Item 2 from file: 696)
DIALOG(R)File 696:DIALOG Telecom. Newsletters
(c) 2003 The Dialog Corp. All rts. reserv.

00662419
E-BUSINESS ISSUES KEEP BANKING CEOs UP AT NIGHT
ELECTRONIC COMMERCE NEWS
March 29, 1999 VOL: 4 ISSUE: 13 DOCUMENT TYPE: NEWSLETTER
PUBLISHER: PHILLIPS BUSINESS INFORMATION
LANGUAGE: ENGLISH WORD COUNT: 460 RECORD TYPE: FULLTEXT

During a Banking Industry Technology Secretariat (BITS) symposium detailing security and trust-building initiatives for e- commerce this month, financial institutions were issued a

(c) PHILLIPS PUBLISHING INTERNATIONAL All Rts. Reserv.

COMPANY NAME(S): American Bankers Association ; ABAecom ; Banking Industry Technology ; BITS ; Telcordia Technologies

TEXT:
...years ago, the CEOs wouldn't have said these things," says Catherine Allen, CEO of BITS.
"The **time** is now [to promote e-commerce security measures], and it's passing those who wait. Applications are...
...Washington-based ABAecom, a for-profit unit of the American Bankers Association that provides electronic authentication and **encryption services** to financial institutions.

Questions Of Direction

A small army of software vendors have tied their futures to...

...protocol - largely ignored by the U.S. banking and e-commerce industries?
"Skeptics are looking at the **cost** of [PKI and other security] infrastructures, and it's a valid point - in the consumer market. It...

...grow," says William Barr, executive director for Morristown, N.J.-based telecom firm Telcordia Technologies.

"But the **time** to invest in business-to-business [e-commerce initiatives] is now, if it's not too late...

12/5,K/9 (Item 3 from file: 696)
DIALOG(R)File 696:DIALOG Telecom. Newsletters

00659383
Items of Interest
Report on Smart Cards
March 15, 1999 VOL: 13 ISSUE: 5 DOCUMENT TYPE: NEWSLETTER
PUBLISHER: BRP PUBLICATIONS
LANGUAGE: ENGLISH WORD COUNT: 966 RECORD TYPE: FULLTEXT

* Visa International March 8 said it would launch the Chip Offline Pre-Authorized Card (COPAC) this year in Ghana. Standard Chartered Bank Ghana plans to issue some 60,000 smart cards under

COMPANY NAME(S): Allied Banks ; Allied Irish Banks ; Bank of Ireland ; Cadence Design Systems Inc ; Norman Access Control ; Norman Data Defense Systems ; PubliCARD Inc ; Samsung Electronics Co Ltd ; Schlumberger Smart Cards & Terminals ; Siemens Semiconductors ; Standard Chartered Bank Ghana ; Sun Microsystems Inc ; Telecom Eireann ; Tritheim Technologies ; VeriFone Inc ; Visa International

TEXT:
...Access, a new smart card based on Java technology that combines multiple application capabilities with built-in **cryptographic services** . Cyberflex Access provides information security services - digital signatures, authentication and authorization - with application security features, such as...

...the power of smart card technology in an open, user- programmable form to help customers cut both **cost** and **time** to market." Schlumberger: http://www.slb.com

12/5,K/10 (Item 4 from file: 696)
DIALOG(R)File 696:DIALOG Telecom. Newsletters

00615450
SUMMARY OF RESPONSES TO THE CONSULTATION PAPER
TELECOMMS FRAUD REVIEW
June 1, 1998 VOL: 2 ISSUE: 6 DOCUMENT TYPE: NEWSLETTER
PUBLISHER: PHILLIPS BUSINESS INFORMATION
LANGUAGE: ENGLISH WORD COUNT: 1080 RECORD TYPE: FULLTEXT

DTI Public Consultation paper on Licensing of Trusted Third Parties for the Provision of Encryption Services produced 260 responses, 129 by conventional mail or fax and 131 by

COMPANY NAME(S): Encryption Services

TEXT:

DTI Public Consultation paper on Licensing of Trusted Third Parties for the Provision of **Encryption** **Services** produced 260 responses, 129 by conventional mail or fax and 131 by e-mail. 102 were from...
...difficulty of defining exclusions.
There were fears that the proposed licensing conditions would be too burdensome and **costly** . A tiered approach was advocated by some, with varying TTP licensing conditions depending on the range of functions offered. There were many pleas from business organisations for the maximum **amount** of freedom to be left to the market, and many expressed confidence that in this fast-changing...session key being handed over or a master key of some kind. If the latter, then any **time** limit specified in the warrant could be ignored.
* The design, implementation and operation of the systems necessary...conveniently
available to them...') was not considered convincing. The conclusion drawn was that the proposals would bring **cost** and complexity to law-abiding users while not necessarily achieving the results the law enforcement authorities want.
...

12/5,K/11 (Item 1 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

03829222 Supplier Number: 48315731 (THIS IS THE FULLTEXT)
IBM TO RELEASE OS/390 VERSION 2 RELEASE 5 IN MARCH
Report on IBM, v15, n8, pN/A
Feb 25, 1998
ISSN: 0742-5341
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 1111
TEXT:
Has Component Broker For Distributed Applications

IBM on Monday announced the March availability of OS/390 Version 2 Release 5, the IBM flagship operating system for IBM S/390 servers. The release is enhanced with features designed to facilitate secure e-business, effective server consolidation and systems management, and application development.

OS/390 is UNIX 95 branded, enabling developers to deploy new UNIX applications or port existing applications from UNIX and other leading application environments to the S/390 platform. OS/390 also is ITAA certified.

The release enhances OS/390 security services with the integration of Triple DES (Data Encryption Standard), a high-level data encryption implementation, the Secure Electronic Transaction (SET) protocol, digital certificates and OS/390 Firewall Technologies. All of the technologies exploit the previously announced IBM S/390 cryptographic coprocessor, a hardware-embedded chip that is standard with the S/390 G4 Enterprise Server, providing customers with better security than can be achieved with software alone, according to IBM.

Tom Rosamilia, director of IBM's S/390 software division, said IBM was "making the safety net wider and stronger" for users who want to conduct business over the Internet.

"IBM is now providing enterprise customers with a significantly enhanced secure Web server with the latest release of OS/390," said David Carlucci, general manager, IBM S/390 Division. "No other platform offers such a wide safety net for intranet, extranet and Internet transactions. By extending our security support to provide extra value to our customers, we have integrated S/390's existing strengths with new and improved technologies."

"IBM has merged the best of what was RACF with the modern security services needed for Web and network computing -- all in the standard release of OS/390," said Jim Hurley, director of information security with Aberdeen Group, a Boston-based consulting group.

"These integrated security services make it possible for users to reuse critical CICS, DB2, IMS and TSO-based applications for critical networked application deployments," Hurley continued. "By providing an integrated set of security services with the release of OS/390, including firewalls, Web servers, a wide variety of authentication credentials, high **speed** and high-strength **cryptographic services** and modern user management tools and interfaces, IBM is defining a new **cost** -effective envelope for decision makers."

S/390 and the OS/390 operating environment are Web-ready, offering three levels of security -- network, system and transaction-level security -- for e-business applications.

Hardware/Software Security

The S/390 cryptographic coprocessor chip, along with the IBM Integrated Cryptographic Services Facility (ICSF), and Triple DES encryption provide more reliable transaction-level security at a higher performance level than customers can obtain with just software. The ICSF has been extended to support SET V1.0, the security protocol developed jointly by Visa International, MasterCard, IBM and others, and is available in March with OS/390.

The ICSF provides cryptographic support for Visa and MasterCard user verification, reducing risk of losses resulting from alteration and counterfeiting of the credit card's magnetic stripe. SET is a standard technology that is used with the IBM CommercePoint products. CommercePoint products exploit the CMOS cryptographic hardware and provide customers with a high level of transaction security.

IBM also integrated security enhancements with OS/390 V. 2 Rel. 5. These include the Lightweight Directory Access Protocol (LDAP), digital certificates, hardware cryptography support for SET and Firewall Technologies.

Enhanced Security

* LDAP. The OS/390 Security Server has been enhanced with LDAP, a new directory service on OS/390 that allows any LDAP client across an enterprise to search, extract and delete information from a directory located on an LDAP S/390 server. With the LDAP capability on S/390, customers now may consolidate directory functions from their distributed environment to S/390, simplifying system management and benefitting from S/390 security.

* Firewall technologies. The Firewall Technologies, available as a kit with OS/390 Version 2 Release 4, is now integrated with OS/390 V. 2 Rel. 5. It works with the cryptographic coprocessor and builds upon existing S/390 security capabilities to offer customers higher levels of protection for network applications by helping to control user access to separate servers inside and outside a network. The Firewall Technologies provides customers with high network security to transact e-business as the firewall screens every piece of data as it enters and leaves a network. The Firewall Technologies also contains a "Virtual Private Network" function designed to allow data to flow securely across a network or between networks.

* Digital certificates. Provide Web browser users accessing the Internet with a signed electronic document that contains information uniquely identifying the user. These digital certificates provide users with a high level of system security. OS/390 Security Server will accept authenticated digital certificates from the Domino Go Webserver and associate that certificate with an OS/390 Security Server user, without

requiring that user to enter a user ID or password. The user then can access OS/390 resources or data.

Commerce Enablement Tools

OS/390 also is allowing customers to conduct business over the Internet with Net.Commerce. In addition, customers can access a S/390 Web server and work with Java.

* Net.Commerce Version 3.0. When used with Domino Go Webserver, Net.Commerce Version 3.0, available with OS/390 V. 2 Rel. 5, will enable customers to set up an Internet presence to showcase products and services to conduct e-business. Domino Go Webserver is a high-performance Web server with full-text search capabilities and dynamic workload balancing. Net.Commerce supports payment transactions using SET and offers Catalog Assistant to help shoppers choose purchases.

* eNetwork Host On-Demand. IBM also announced eNetwork Host On-Demand Version 2 for S/390, software that allows any Java-enabled client to access a Web server on S/390 and download a 100 percent pure Java applet. The end user then can access any host on a network, without the need for an intermediate server. Support of Java applets is centralized on one platform making working with Java easy.

Component Broker for OS/390

OS/390 also is offering to selected customers a beta of Component Broker for OS/390. Component Broker masks the complexity of enterprise computing by tying together disparate systems found in today's Fortune 500 companies via an object framework, thereby letting customers focus on their core businesses rather than writing code. Now available on Windows NT as a comprehensive solution of software, services and education, Component Broker is comprised of Component Broker Connector (CBConnector) and the supporting Component Broker Toolkit (CBToolkit). At completion of the beta program later this year, Component Broker for OS/390 will be available for OS/390 V. 2 Rel. 5 and OS/390 Version 2 Release 6 customers.

PUBLISHER NAME: DataTrends Publications, Inc.
INDUSTRY NAMES: BUSN (Any type of business); CMPT (Computers and Office Automation)

... with the release of OS/390, including firewalls, Web servers, a wide variety of authentication credentials, high **speed** and high-strength **cryptographic services** and modern user management tools and interfaces, IBM is defining a new **cost** -effective envelope for decision makers."

S/390 and the OS/390 operating environment are Web-ready, offering...

12/5,K/12 (Item 2 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2003 The Gale Group. All rts. reserv.

03828862 Supplier Number: 48315087 (THIS IS THE FULLTEXT)
IBM: IBM offers S/390 customers wider safety net to conduct e-business
M2 Presswire, pN/A
Feb 25, 1998
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 949
TEXT:
M2 PRESSWIRE-25 February 1998-IBM: IBM offers S/390 customers wider safety net to conduct e-business (C)1994-98 M2 COMMUNICATIONS LTD

RDATE:230298

IBM today announced the industry's premier system security for conducting business over the Internet. This leading security comes from a one-two punch of a software/hardware solution integrated with IBM's flagship enterprise operating system, OS/390, and IBM S/390 Parallel Enterprise servers - Generation 3 and Generation 4.

IBM also announced enhancements to OS/390 that will provide customers with higher levels of performance for UNIX, Web serving and traditional applications, a server consolidation solution for enhanced print server management and improved application development. At the heart of today's announcement is OS/390 Version 2 Release 5, available in March.

"IBM is now providing enterprise customers with a significantly enhanced secure Web server with the latest release of OS/390," said David Carlucci, general manager, IBM S/390 Division. "No other platform offers such a wide safety net for intranet, extranet and Internet transactions. By extending our security support to provide extra value to our customers, we have integrated S/390's existing strengths with new and improved technologies."

S/390 and the OS/390 operating environment can provide customers with three critical levels of security -- network, system and transaction-level security -- for e-business applications. S/390's set of system integrity, resource control, cryptographic and network security features, combined with existing S/390 classic strengths, bring customers a Web-ready server solution with no need to reinvest in a totally new infrastructure to launch e-business applications.

This OS/390 release highlights significant enhancements to the OS/390 security services with the integration of Triple DES (Data Encryption Standard), a high-level data encryption cryptographic standard. IBM's offering of Triple DES, like standard DES, exploits the previously announced IBM S/390 cryptographic coprocessor, a hardware- embedded chip standard with the S/390 G4 Server. Triple DES integration is unique within IBM to the S/390 G4 servers. Triple DES is available in accordance with applicable country export regulations.

IBM Offers High Level Data Protection

Triple DES, with the hardware cryptographic coprocessor, is designed to provide customers with exponentially stronger encryption protection than what standard DES or software alone currently offers. Triple DES, critical for financial institutions, is based on DES, a reliable standard for network and information security for the past 20 years.

In addition to Triple DES, IBM today announced extensions to its industry-leading security beyond the OS/390 Security Server, formerly known as Resource Access Control Facility (RACF) and Distributed Computing Environment (DCE), to make it easier for customers to extend their rock-solid security model to e-business and server consolidation. These security enhancements, integrated with OS/390 V. 2 Rel. 5, include the Lightweight Directory Access Protocol, digital certificates, hardware cryptography support for the Secure Electronic Transaction (SET) protocol and Firewall Technologies.

"IBM has merged the best of what was RACF with the modern security services needed for Web and network computing -- all in the standard release of OS/390," said Jim Hurley, director of information security with Aberdeen Group, a Boston- based consulting group.

"These integrated security services make it possible for users to reuse critical CICS, DB2, IMS and TSO-based applications for critical networked application deployments," Hurley continued. "By providing an integrated set of security services with the release of OS/390, including firewalls, Web servers, a wide variety of authentication credentials, high **speed** and high-strength **cryptographic** **services** and modern user management tools and interfaces, IBM is defining a new **cost** -effective envelope for decision makers."

High Performance Connectivity and Web Access

In addition to premier Web security offerings, S/390 made its Web server a world-class performer. IBM significantly redesigned the TCP/IP services in OS/390 eNetwork Communications Server to take full advantage of the performance and scalability of the S/390 servers. These new TCP/IP services will enable UNIX, Web serving and traditional applications to benefit from improved performance, function and increased connectivity bandwidth with native

ATM and Fast Ethernet. For high demand S/390 Web serving environments, the High Speed Web Access service is included.

Internal IBM performance tests using High Speed Web Access with OS/390's Domino Go Webserver 4.6 have measured a ten-fold improvement in Web connections per second -- more than 3,000 connections. The improved speed means the customer's S/390 Web server could handle more than 200 million Internet hits a day.

Server Consolidation

While OS/390 V. 2 Rel. 5 offers customers security and connectivity performance improvements, the new release also allows customers to consolidate workloads on a single S/390 platform, helping reduce complexity and operating costs, and improve manageability. The new OS/390 Print Server can handle both host and LAN printing for native UNIX applications and TCP/IP connected clients, eliminating the need for multiple print servers enterprisewide. Customers can specify any printer connected to the S/390 server to handle the print job.

Component Broker for OS/390

OS/390 V. 2 Rel. 5 also is offering to selected customers a beta version of Component Broker for OS/390. Component Broker for OS/390 is IBM's enterprise solution for distributed object computing, providing a scalable, manageable run-time for developing and deploying multi-tier component-based applications.

OS/390, S/390 Parallel Enterprise Server Generation 3 and Generation 4, IBM, RACF, CICS, DB2 and Component Broker are trademarks or registered trademarks of International Business Machines Corporation.

Domino Go Webserver is a trademark of Lotus Development Corporation.

UNIX is a registered trademark of The Open Group.

All others are trademarks or registered trademarks of their respective companies.

M2 COMMUNICATIONS DISCLAIMS ALL LIABILITY FOR INFORMATION PROVIDED WITHIN M2 PRESSWIRE. DATA SUPPLIED BY NAMED PARTY/PARTIES.

PUBLISHER NAME: M2 Communications
INDUSTRY NAMES: BUSN (Any type of business); INTL (Business, International)

... with the release of OS/390, including firewalls, Web servers, a wide variety of authentication credentials, high **speed** and high-strength **cryptographic services** and modern user management tools and interfaces, IBM is defining a new **cost** -effective envelope for decision makers."

High Performance Connectivity and Web Access

In addition to premier Web security...

12/5,K/13 (Item 3 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2003 The Gale Group. All rts. reserv.

03828150 Supplier Number: 48313072 (THIS IS THE FULLTEXT)
IBM: IBM offers customers wider safety for e-business on the Internet
M2 Presswire, pN/A
Feb 24, 1998
Language: English Record Type: Fulltext

Document Type: Newswire; Trade
Word Count: 881
TEXT:

M2 PRESSWIRE-24 February 1998-IBM: IBM offers customers wider safety for e-business on the Internet (C)1994-98 M2 COMMUNICATIONS LTD

RDATE:230298

IBM today announced extensions to its OS/390 operating system that greatly improve the security of transacting business over the Internet for banks and financial institutions. This industry-leading security comes from unique features of IBM S/390 hardware that are exploited by OS/390 Version 2 Release 5, which is available in March. Also announced are enhancements to the operating system that will provide customers with higher levels of performance for UNIX and Web serving, a server consolidation solution for managing network printing, and the availability of new application development tools.

OS/390 V2.5 features new system security from its integration of Triple DES (Data Encryption Standard). IBM's Triple DES, like standard DES, exploits the previously announced IBM S/390 cryptographic coprocessor, a hardware embedded chip that is standard with the IBM S/390 Parallel Enterprise Server -- Generation 4 and is unique within IBM to the S/390 G4 servers. Outside North America, Triple DES will require licensing in compliance with U.S. export regulations.

The S/390 cryptographic coprocessor chip, along with the IBM Integrated Cryptographic Services Facility (ICSF) and Triple DES encryption provide customers with far stronger encryption protection than standard DES or software alone currently offers. In addition, the ICSF has been extended to support SET Version 1.0, the security protocol developed jointly by Visa International, MasterCard, IBM and others. The ICSF and SET provide cryptographic support for Visa and MasterCard user verification, reducing the risk of losses resulting from alteration and counterfeiting of the card's magnetic stripe.

In addition to Triple DES, IBM today announced extensions to its industry-leading security, beyond the OS/390 Security Server, formerly known as Resource Access Control Facility (RACF) and Distributed Computing Environment (DCE) security functions, to make it easier for customers to extend their rock-solid security model to e- business and server consolidation. These security enhancements, integrated with OS/390 V. 2.5 include the Lightweight Directory Access Protocol, digital certificate, hardware cryptography support for SET protocol and Firewall Technologies.

"IBM has merged the best of what was RACF with the modern security services needed for Web and network computing -- all in the standard release of OS/390," said Jim Hurley, director of information security with Aberdeen Group, a consulting group based in Boston, U.S.A.

"These integrated security services make it possible for users to reuse critical CICS, DB2, IMS and TSO-based applications for critical networked application deployments," Hurley continued. "By providing an integrated set of security services with the release of OS/390, including firewalls, Web servers, a wide variety of authentication credentials, high **speed** and high-strength **cryptographic** **services** and modern user management tools and interfaces, IBM is defining a new **cost** -effective envelope for decision makers."

High Speed Web Access

IBM has also significantly redesigned the TCP/IP services in OS/390 eNetwork Communications Server to take full advantage of the performance and scalability of the S/390 servers. These new TCP/IP services will enable UNIX, Web serving and traditional applications to benefit from improved performance, function and increased connectivity bandwidth with native ATM and Fast Ethernet. For high demand S/390 Web serving environments, the High Speed Web Access service is included.

Internal IBM performance tests using High Speed Web Access with

OS/390's Domino Go Webserver 4.6 have measured a ten-fold improvement in Web connections per second -- more than 3,000 connections. The improved speed means the customer's S/390 Web server could handle approximately 200 million Internet hits a day.

Server Consolidation

OS/390 2.5 also allows users to consolidate print workloads on a single S/390 platform, helping reduce complexity and costs. The new OS/390 Print Server can handle both host and LAN printing for native UNIX applications and TCP/IP connected clients, eliminating the need for multiple print servers enterprise-wide. Customers can specify any network printer connected to the S/390 server to handle the print job.

Component Broker for OS/390

As previously announced OS/390 2.5 also is offering selected customers a beta version of Component Broker for OS/390, a new programming tool intended to help users to rapidly design and develop new applications using object-oriented technology. At completion of the beta programme later this year, Component Broker for OS/390 will be available for OS/390 V.2.5. It is expected to be general available, at no additional charge, as part of OS/390 Version 2 Release 6 in September this year.

OS/390, S/390 Parallel Enterprise Server Generation 3 and Generation 4, IBM, RACF, CICS, DB2 and Component Broker are trademarks or registered trademarks of IBM Corporation.

Domino Go Webserver is a trademark of Lotus Development Corporation. UNIX is a registered trademark of The Open Group in the US and other countries. All others are trademarks or registered trademarks of their respective companies.

CONTACT: Diane Whitehead, IBM EMEA S/390 Tel: +44 (0)1256 341256 e-mail: diane whitehead@uk.ibm.com Lorna Campbell, Campbell Communications Tel: +44 (0)1844 338 145 e-mail: lorna@lornac.demon.co.uk

M2 COMMUNICATIONS DISCLAIMS ALL LIABILITY FOR INFORMATION PROVIDED WITHIN M2 PRESSWIRE. DATA SUPPLIED BY NAMED PARTY/PARTIES.

PUBLISHER NAME: M2 Communications
INDUSTRY NAMES: BUSN (Any type of business); INTL (Business, International)

... with the release of OS/390, including firewalls, Web servers, a wide variety of authentication credentials, high **speed** and high-strength **cryptographic services** and modern user management tools and interfaces, IBM is defining a new **cost** -effective envelope for decision makers."

High Speed Web Access

IBM has also significantly redesigned the TCP/IP...

12/5,K/14 (Item 4 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2003 The Gale Group. All rts. reserv.

02588907 Supplier Number: 45233401 (THIS IS THE FULLTEXT)
IT SECURITY IN THE FINANCIAL SECTOR
Computer Fraud & Security Bulletin, pN/A
Jan, 1995
ISSN: 0142-0496
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 2459
TEXT:
Chris Amery Zergo Ltd Computer systems are arguably less secure today than

ever before. This is because they are inherently more complex. Just about all sectors have enthusiastically embraced distributed computing in its many forms. Local and wide area networks now proliferate, linked to large numbers of desktop terminals. Nowhere is this more so than in the financial sector. Banks and insurance companies have rolled out large numbers of networked PCs throughout their branch networks. As a result, more and more sensitive data now passes between the branch and head office. Sales staff and senior managers are increasingly equipped with portable PCs. Huge amounts of money are now transmitted in electronic form every day on a national and international basis. True 24-hour trading, including electronic matching and settlement, is now a reality. Self-service banking is also on the increase as banks seek alternative ways to deliver products. This consists of anything from the ubiquitous automated teller machine to unmanned, fully automated branches. The same forces are driving the provision of remote links to retail customers in the form of home banking services and to corporate customers for enquiry and trade generation purposes. For the future, many banks are currently evaluating the selling and marketing opportunities offered by the much hyped 'information superhighway' or new technologies such as interactive CDs (CD-I). Of course, not so long ago all data and all of the applications used to reside on a big mainframe in the data centre. Now, however, it is the network that is at the heart of every financial organization's IT infrastructure. But every node and every PC on the network represents a potential security risk. PCs and operating systems such as DOS and Unix were not designed with security in mind and are therefore inherently insecure. So too network protocols such as TCP/IP and network types such as X.25, Ethernet, Token Ring, and, in particular, dial-up circuits. Without added security there is no way to ensure that data is accessed only by those authorized to do so. Even less secure is the Internet which was designed very much with openness in mind. It arose from higher education and was intended as a bulletin board which everyone could access. Companies which now have gateways onto the Internet are potentially opening the door to the outside world. So how great are the risks and what should financial organizations be doing to counter them? There are many potential threats, of which hacking and viruses generate the most publicity. The fear that these breed is reflected in the fact that some previous hackers now make a healthy living out of consultancy work. For instance, Chris Googans, who was arrested when he was 15 for being a member of the notorious Legion of Doom hacking group, recently captured the attention of an audience of IT security managers in the UK. He told them that only a very small minority of hackers are ever caught, that hackers are now driven increasingly by a desire to make money (a particular worry to banks, therefore), and that hackers are clearly very technically adept but that often they infiltrate systems by exploiting poor administrative procedures. In fact, internal staff are likely to pose an even greater threat. The recently publicized case of sensitive security telephone numbers from a British Telecom database finding their way onto the Internet is now thought to have stemmed not from hacking but from infiltration by a journalist working as a temporary employee within BT. Over one third of security breaches are deliberate but the majority of these are as a result of fraudulent or malicious behaviour by existing or former staff. Equally serious is the threat of accidental causes whether through the failures of hardware, software, networks or humans. Errors by the latter cannot be viewed in isolation. There is a known example of a human operator at a bank entering an incorrect data parameter. This resulted in a number of foreign exchange and money market deals on a ledger being wrongly posted. The bank's own portfolio could not be managed for two days while it sorted out the mess. The operator should not have typed in the wrong data parameter, but the system should not have been able to accept it. Another significant threat is systems' downtime, for whatever reason. It is virtually impossible to measure the overall **cost** of security breaches to the financial services industry. Much of it still goes unreported. It is also difficult to define. If someone has just withdrawn money from an ATM and is then mugged, should this be included in the statistics? How about if that person has the ATM card itself stolen? Five different surveys will come up with five different answers, none of which are likely to be much help in combating the problem. What can be said is that the problem seems to be on the increase. A recent report by the Audit Commission found that the number of reported computer abuse incidents from over 1000 organizations almost tripled between 1990 and 1993. So what should financial organizations do to counter the threats? Firstly, fundamentally, they need to identify and quantify the threats. Where are the weaknesses in the systems and procedures? There should be regular internal and external audits which adopt a methodical and independent approach to this issue, taking in asset identification and valuation, threat and vulnerability assessment, testing where applicable, and the production of baseline control reports. The review might well be based on an existing methodology such as CRAMM. The task should encapsulate not only the systems but also considerations such as building security, staff vetting, business continuity planning and backup procedures. Responsibility for security policy and coordination should be specifically allocated to members of staff. Security evaluation must also be an on-going job involving continuous assessment of the problems and solutions. After all, the pace of change within most financial services organizations means that the underlying systems themselves are constantly changing. A key part of any organization's security structure is the need for integrated, comprehensive documentation which sets out the security policy and all related standards, practices, products and procedures. Barclays Bank has recently produced such a study which is intended to define the specific security measures across the entire bank. This sort of initiative is linked to the need for senior management to demonstrate its full and explicit support for security policies. This is important because security is likely to inconvenience staff and can generate hostility. Employees must be made to understand the importance of security and must be aware of senior commitment to the cause. After all, staff are a key element in making systems and organizations more secure. They need to be vigilant and should be encouraged to report any suspicious circumstances. Indeed, this is now being enforced in some quarters. The European Union's money laundering directive is being implemented in the UK within the Money Laundering Regulations and Criminal Justice Act. This introduces a number of offenses including failure to disclose information to the police if someone knows or suspects that another person is engaged in drug money laundering. This is particularly applicable to the back office staff of banks who are now legally obliged to report any suspicious circumstances. Ultimately no one can afford to make any system 100% secure. The key issue is to identify the areas of greatest risk and ensure that these are effectively managed. When weighing the potential losses against the **cost** of security it is important to consider this within the context of the overall business. For instance, if an ATM network is breached then a financial loss will be incurred, but a potentially much more damaging result will be a loss of confidence among existing and potential customers. Other considerations include the fact that security measures may impact the performance of the systems and organization itself. It is no good making a system virtually watertight if it grinds to a halt as a result. Security measures may also inconvenience customers. For instance, a number of banks now say that their customers must collect new ATM cards and/or PINs from their branch. This is clearly more secure than sending the cards and numbers through the post, but it does inconvenience the customer. As a result, those banks that have adopted such a policy are still in the minority. Similarly, it is widely accepted that PINs are not particularly secure. However, they are convenient. From a technical point of view, it is perfectly feasible to introduce security based on retina scans, signature verification, fingerprint reading and the like but not only are these still potentially very **costly** they may also not be acceptable to the majority of customers. There is a very wide range of security solutions available of which some of the more common include passwords, keys, tokens, smartcards, encryption and authentication, and artificial intelligence for identifying anomalies in credit usage for instance. Indeed, there is so much going on in this market that it is difficult to keep up with the changes. Here, as elsewhere, most organizations are likely to need help from security specialists. New approaches and techniques for security are being defined every month, new products are continually coming onto the market, and standards are slowly starting to appear. Pressure is also growing from outside forces including regulators such as central banks, which carry out regular audits. Banks must also give careful consideration to the implications of the Consumer Protection Act. New legislation is also currently being demanded by the European Union. One area which is particularly worthy of attention is that of application security. Users often assume that adequate security has been built in at the design stage, but this is seldom the case. One possible solution is to attack the problem at the software design stage. This is being done by NatWest Bank, for instance, which is providing all of its systems and applications developers with a risk assessment tool. Incorporating elements of artificial intelligence, the tool allows the bank to weight risk based on past experiences and statistical analysis. Users can drill down through the data and are provided with risk assessments measured by a range of criteria. It is clearly not a panacea but it does place the emphasis for security on to the systems and applications developers themselves. They are not security specialists and are usually fighting against tight deadlines and budgets, often unsuccessfully. It is easy to ignore security in the race to meet pressing business requirements. The NatWest approach works for new in-house applications development but what about security legacy and packaged software sourced from third party vendors? In terms of the latter, the UK Government is putting a lot of emphasis on a formal evaluation and certification based on the European ITSEC initiative. The first ITSEC criteria were published in mid 1991 and are intended for use in evaluating the security of products and systems. The ITSEC criteria have not been widely used outside the public sector, mainly because they have been found to be too formal, too **time** -consuming and too expensive and the new Common Criteria being developed jointly in Europe, USA and Canada may not be an improvement in that respect. Some form of testing and evaluation is important, but, for the **time** being at least, the ITSEC criteria seem to be less practical than those offered by some security specialists. With regard to the more technical aspects of system security, there is a strong argument for services to be handled centrally rather than in the application. It is a more flexible approach in that the security aspects do not have to be written from scratch for every new application. Systems can be changed and new applications can be added without significantly impacting overall security. It also ensures consistency, allowing users to dispense with the inefficiencies of trying to support different approaches to security for different applications. The high **cost** of the monolithic approach has restricted the use of **cryptographic services** to only the most critical applications, often forcing companies to accept levels of risk that are greater than can be justified. Where the two are detached, the security facilities, such as those for ensuring the confidentiality and integrity of data, reside on a server. The application effectively becomes the client, calling the relevant security facilities as required via standard programming interfaces (APIs). The security facilities can be bought in an off-the-shelf, modular fashion and can significantly reduce development and implementation times an important consideration in ever more competitive markets. The benefits of such an approach are currently being reaped by the

Italian banking community among others. CIPA, the strategic committee representing all of the major Italian banks, carried out a review of IT procedures. Out of this came a plan to implement additional security across the inter-bank, X.25 network. Secure messaging is now provided through easy to use encryption keys which are distributed at appropriate levels. There are over 200 banks on the network and these use a vast array of applications. The security services reside on servers and are therefore detached from the disparate bank systems. As a result, there have been considerable **cost** savings and the majority of system operations are transparent to the user, with a common look-and-feel provided regardless of the underlying platform. Awareness of the problems and possible solutions is growing, but there is still a stigma surrounding the whole area of security, especially in a sector as sensitive as finance. This is one reason why so many breaches go unreported. The fear of bad publicity and undermining public confidence are powerful influences. This means that lessons are not shared and everyone is left to tackle the thorny questions of systems security more or less in isolation although user groups like the European Security Forum can be very effective as 'multipliers' of experience and good practice. One indication that computer security may be coming out of the closet at last is the recent setting up of Europe's first specialized postgraduate diploma in information technology security. This has been developed by Royal Holloway, University of London, in conjunction with Zergo Ltd. It is designed to provide theoretical expertise. Key rates of study include cryptography, network security, systems security, and information security management. As companies continue to invest in new technology and continue to roll out new systems, the security implications must be taken into consideration from the outset. It is vital that financial services organizations take a thorough and methodical approach to systems security. It should be an on-going, centrally coordinated task involving regular health checks, reviews and audits. Security can no longer be treated as an after thought, it must be a core component of all systems planning.

PUBLISHER NAME: Elsevier Science, Inc.

INDUSTRY NAMES: BUSN (Any type of business); CMPT (Computers and Office Automation); GOVT (Government and Law); INTL (Business, International)

(USE FORMAT 7 FOR FULLTEXT)

TEXT:

...Another significant threat is systems' downtime, for whatever reason. It is virtually impossible to measure the overall **cost** of security breaches to the financial services industry. Much of it still goes unreported. It is also...of greatest risk and ensure that these are effectively managed. When weighing the potential losses against the **cost** of security it is important to consider this within the context of the overall business. For instance...

...retina scans, signature verification, fingerprint reading and the like but not only are these still potentially very **costly** they may also not be acceptable to the majority of customers. There is a very wide range...

...widely used outside the public sector, mainly because they have been found to be too formal, too **time** -consuming and too expensive and the new Common Criteria being developed jointly in Europe, USA and Canada...

...be an improvement in that respect. Some form of testing and evaluation is important, but, for the **time** being at least, the ITSEC criteria seem to be less practical than those offered by some security...

...dispense with the inefficiencies of trying to support different approaches to security for different applications. The high **cost** of the monolithic approach has restricted the use of **cryptographic services** to only the most critical applications, often forcing companies to accept levels of risk that are greater...

...servers and are therefore detached from the disparate bank systems. As a result, there have been considerable **cost** savings and the majority of system operations are transparent to the user, with a common look-and...

12/5,K/15 (Item 5 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2003 The Gale Group. All rts. reserv.

02437257 Supplier Number: 44857780 (THIS IS THE FULLTEXT)
PRODUCT NEWS
Network Week, n132, pN/A
July 22, 1994
ISSN: 0965-3031
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 371
TEXT:
Motorola Inc's Wireless Data Group says it is now targeting the end of the year for shipment of the Envoy personal wireless communicator as a result of extended testing. Envoy, based on General Magic Corp's Magic Cap communicating applications system and Telescript communications language, is the first hand-held device to feature three types of communications. Houston, Texas-based LAN Support Group has launched NetSqueeze and NetSqueeze+Encryption, NetWare Loadable Modules said to provide file compression and **encryption services** for NetWare 3.x and 4.x file servers. According to the company, NetSqueeze provides real- **time** , transparent compression. It claims that the offering increases file storage capacity by up to 60%. NetSqueeze+ Encryption encrypts files before they are compressed, and allows administrators to keep private files on NetWare servers, says the company. It also reportedly enables administrators to specify which users can use **encryption services** . Each module lists for $250 and will ship from September in the US. Tucson, Arizona-based Artisoft Inc has added a new option to its entry- level version of the LANtastic operating system, Simply LANtastic (Network Week, 096), in the form of add-on kits with new parallel port adapters. The kits are available immediately, **costing** $179. The move is designed to allow users to tie laptop computers into their Simply LANtastic networks. Milton Keynes-based Psion Dacom has announced a new ISA adapter designed to allow users of its PCMCIA-based Gold Card modem range to use their modems within ISA-based desktop computers: the company believes that, rather than opting for two modems for desktop and laptop machines, users will want to double-up and share modems between the two types of computer. The 8 bit ISA half card is to **cost** 50 when bought with a Psion Gold Card modem, or 99 purchased separately. Sun Microsystems Computer Co is shipping the SunFastEthernet switchable 10/100Mbps 100Base-T "Fast Ethernet" adaptor. The onboard 100Base-TX transceiver enables the adaptor to run over two-pair Category 5 UTP wiring while the Media Independent Interface, when connected to an external third-party transceiver, enables the adaptor to run over additional wiring types, including fibre, STP and four-pair Category 3 and 4 UTP wiring. The single-wide card uses the core CSMA/CD protocol of IEEE 802.3; it **costs** $800.

COPYRIGHT 1999 Gale Group
PUBLISHER NAME: ComputerWire, Inc.
COMPANY NAMES: *LAN Support Group Inc.; Motorola Inc.; Psion Dacom; Sun Microsystems Inc.
EVENT NAMES: *330 (Product information)
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *7372620 (Network Software); 3661271 (Data Modems); 3661257 (LAN/WAN Adapters); 3662152 (Ground Mobile Radio Systems)
INDUSTRY NAMES: BUSN (Any type of business); CMPT (Computers and Office Automation); INTL (Business, International)
NAICS CODES: 51121 (Software Publishers); 334418 (Printed Circuit Assembly (Electronic Assembly) Manufacturing); 33421 (Telephone Apparatus Manufacturing); 33422 (Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing)
TICKER SYMBOLS: MOT; SUNW

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...Support Group has launched NetSqueeze and NetSqueeze+Encryption, NetWare Loadable Modules said to provide file compression and **encryption services** for NetWare 3.x and 4.x file servers. According to the company, NetSqueeze provides real- **time** , transparent compression. It claims that the offering increases file storage capacity by up to 60%. NetSqueeze+ Encryption...

...on NetWare servers, says the company. It also reportedly enables administrators to specify which users can use **encryption services** . Each module lists for $250 and will ship from September in the US. Tucson, Arizona-based Artisoft...

...in the form of add-on kits with new parallel port adapters. The kits are available immediately, **costing** $179. The move is designed to allow users to tie laptop computers into their Simply LANtastic networks...

...and share modems between the two types of computer. The 8 bit ISA half card is to **cost** 50 when bought with a Psion Gold Card modem, or 99 purchased separately. Sun Microsystems Computer Co...

...UTP wiring. The single-wide card uses the core CSMA/CD protocol of IEEE 802.3; it **costs** $800.

12/5,K/16 (Item 1 from file: 813)
DIALOG(R)File 813:PR Newswire
(c) 1999 PR Newswire Association Inc. All rts. reserv.

1209519 LAM048
RSA Launches Field Trial of BSAFE 4.0 With Elliptic Curve Technology

DATE: January 12, 1998 08:04 EST WORD COUNT: 1,146

SAN FRANCISCOJan. 12 /PRNewswire/ -- -- -- RSA DATA SECURITY CONFERENCE -- Software developers will now be able to get first-hand experience with elliptic curve cryptography (ECC) as RSA Data Security, Inc., today launched a field trial of the latest version of its BSAFE(TM) toolkit and encryption engine. The BSAFE 4.0 engine marks the introduction of elliptic curve technology to RSA's product line, giving developers who want to begin researching and prototyping solutions using this technology the ability to do so using the familiar BSAFE API.

Elliptic curve cryptosystems have a number of properties that make them attractive tools for meeting the security requirements of a growing number of applications, but the technology has yet to be subjected to broadly-based scrutiny from the developer community. RSA believes the scope of this field trial will play an important role in fostering an evaluation of the effectiveness of ECC technology. RSA's goal is to have ECC-enabled trial BSAFE toolkits in the hands of at least 50 selected developers by the second quarter of 1998. Participation in the field trial is free.

Initial members of the field trial include ASIC International, Atalla Corp., Intel Corporation, Microsoft Corporation, Netscape Communications Corporation, Network Computer, Inc., Rainbow Technologies, Inc., Security Dynamics Technologies, Inc., Verifone, Inc. and VeriSign, Inc.

"While many public-key cryptosystems proposed over the years have been broken or found to be too costly, elliptic curve cryptosystems appear promising at this point and deserve further analysis," said Jim Bidzos, president of RSA Data Security. "Our focus has always been on providing the right cryptographic technology to suit the diverse needs of our customers."

"Microsoft is pleased to see the increasing choice of cryptographic technologies to satisfy the diverse needs of our customers such as Elliptic Curve Cryptography as found in BSAFE 4.0," said Barbara Fox, Security Architect at Microsoft. "Developers can use the Microsoft CryptoAPI framework and choose from the large number of Cryptographic Service Providers available from ISVs for integrating different cryptographic algorithms into their applications."

"Security is among the most important issues facing developers as they design and deploy intranets and extranets," said Taher ElGamal, chief scientist at Netscape Communications Corporation. "This broad-based market trial will provide the development community with the real-world experience needed to understand and realize the full potential of elliptic curve technology."

The BSAFE engine, an industry leading encryption engine with more than 300 million copies embedded in developer applications, reduces the **time** , costs, and complexity associated with the development of secure applications. The BSAFE engine is designed to provide developers with the security components they need for a wide range of applications, including digitally signed forms, private Internet communications, signed, tamperproof applications, secure wireless communications, and virtual private networks. The RSA-base **Cryptographic Service** Provider for Microsoft's CryptoAPI is based on BSAFE.

ECC cryptosystems are especially attractive for applications such as embedded systems where memory size and processing power are limited. The elliptic curve functions in the BSAFE 4.0 engine include the generation of EC parameters, computation and verification of EC DSA signatures, and EC Diffie- Hellman key agreement following IEEE P1363, as well as an ECC encryption scheme. The BSAFE 4.0 engine is designed to provide support for all three types of elliptic curve cryptography, including so-called "odd," "even- normal," and "even polynomial" variants. The BSAFE 4.0 engine also provides data compression functions, an open hardware interface for running cryptographic accelerators under BSAFE API, and compliance with the emerging ANSI X9 series of public key standards for the financial industry. Eventually BSAFE 4.0 will integrate with other RSA products, such as the recently announced Certificate Security Suite(TM), which is based on the CDSA specification and would support ECC as a cryptographic service provider.

The BSAFE 4.0 toolkit continues to include standard public key algorithms such as RSA, DSA and Diffie-Hellman; a wide range of symmetric encryption algorithms, including RC2, RC4, RC5, DES and Triple DES; as well as message digest algorithms MD2, MD5 and SHA-1. Important security components such as password-based encryption, random number generation and Bloom-Shamir secret sharing are also provided.

"Scrupulous crypto-analysis of ECC is still in its infancy," said Scott Schnell, RSA's vice president of marketing. "But the BSAFE 4.0 encryption engine prepares developers for a number of opportunities by offering implementations for use today and for tomorrow's possibilities."

While elliptic curve cryptography is not yet in significant commercial use, RSA has been involved for several years in the standardization of elliptic curve cryptosystems as part of the IEEE P1363 project, and in developing elliptic curve technology through its RSA Laboratories division and also in partnership with the State key Laboratory of Information Security (LOIS) of the People's Republic of China. RSA Laboratories maintains an ongoing program of studying new techniques for efficient implementation of ECC and other cryptosystems and standards to ensure robustness and interoperability of resulting applications.

Sign-up for the Beta program will begin on Wednesday, January 14 at the RSA booth, RSA Data Security Conference. Developers wishing to participate in the field trial of the BSAFE 4.0 encryption engine may also visit the RSA Developers' Corner section of RSA's Web site at http://www.rsa.com/rsa/developers/, or contact Jeremy Steiglitz at 650-595-8782.

About RSA Data Security, Inc.

RSA Data Security, Inc., a wholly owned subsidiary of Security Dynamics Technologies, Inc. (Nasdaq: SDTI), is a leading supplier of software components that secure electronic data, with more than 300 million copies of RSA encryption and authentication technologies installed worldwide. RSA technologies are part of existing and proposed standards for the Internet and World Wide Web, ISO, ITU-T, ANSI, IEEE, and business, financial and electronic commerce networks around the globe. RSA develops and markets platform- independent security components and related developer kits and provides comprehensive cryptographic consulting services. RSA can be reached at http://www.rsa.com.

BSAFE and Certificate Security Suite(TM) are trademarks of RSA Data Security, inc. All other product or brand names are trademarks or registered trademark of their respective owners.

This press release contains forward-looking statements relating to the planned market trial and release by RSA Data Security, Inc. of its BSAFE 4.0 developer's toolkit and encryption engine and such statements involve a number of risks and uncertainties. Among the important factors that could cause actual results to differ materially from those indicated by such forward- looking statements are delays in product development, undetected software errors or bugs, competitive pressures, technical difficulties, general economic conditions and the risk factors detailed from time to time in Security Dynamics' periodic reports and registration statements filed with the Securities and Exchange Commission, including without limitation Security Dynamics' Registration Statement on Form S-3, as amended (File No. 333-35035), filed on September 5, 1997.

SOURCE RSA Data Security, Inc.

CONTACT: Patrick Corman of Corman Communications, 650-326-9648 or corman cerfnet.com

Web site: http://www.rsa.com

(SDTI)

```
COMPANY NAME:    RSA DATA SECURITY, INC.
TICKER SYMBOL:   SDTI (NDQ)
PRODUCT:         COMPUTER, ELECTRONICS (CPR); INTERNET, MULTIMEDIA,
                    ONLINE (MLM)
DESCRIPTORS:     NEW PRODUCTS & SERVICES (PDT)
STATE:           CALIFORNIA (CA)
SECTION HEADING: BUSINESS; TECHNOLOGY
```

... an industry leading encryption engine with more than 300 million copies embedded in developer applications, reduces the **time** , costs, and complexity associated with the development of secure applications. The BSAFE engine is designed to provide...

... forms, private Internet communications, signed, tamperproof applications, secure wireless communications, and virtual private networks. The RSA-base **Cryptographic Service** Provider for Microsoft's CryptoAPI is based on BSAFE.

ECC cryptosystems are especially attractive for applications such...

12/5,K/17 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2003 The Gale Group. All rts. reserv.

04644019 Supplier Number: 46832624 (USE FORMAT 7 FOR FULLTEXT)
RACAL INTRODUCES SNMP-MANAGED SECURE DATA PROTECTION FOR FRAME RELAY NETWORKS WITH THE DATACRYPTOR 64F ENCRYPTOR
News Release, pN/A
Oct 28, 1996
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 998
PUBLISHER NAME: Various
COMPANY NAMES: *Racal Corp.
EVENT NAMES: *330 (Product information)
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *3662367 (Antitheft Devices NEC)
INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)
NAICS CODES: 33429 (Other Communications Equipment Manufacturing)
SPECIAL FEATURES: COMPANY

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...sNMP device is the lowest priced frame relay SNMP encryptor on the market today, with a list **price** of $2,995. The product is approved for use throughout North and South America and Europe; and...

...64F frame relay encryptor offers an economical alternative to T1/E1 encryptors when used for the lower **speed** 56/64Kbps circuits that constitute the vast majority of frame relay connections. GLOBAL APPLICATION Potential users of...

...for optimum security. Under user control, selected connections can be encrypted while others are not, saving the **cost** of installing encryption devices at frame relay sites that do not require security. The Datacryptor 64F frame...

...is assured of secure key distribution and control. Key changes can be performed automatically without operator Intervention. **Cryptographic service** messages are authenticated with a secure protocol ensuring information integrity. BUILT-IN FEATURES Racal has designed the...

...character display provides valuable information on equipment status, including operating mode, active alarms and the date and **time** of important network events. The Data Link Connection Identifiers (DLCI's), which identify secured and unsecured virtual...

12/5,K/18 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2003 The Gale Group. All rts. reserv.

04258545 Supplier Number: 46236946 (USE FORMAT 7 FOR FULLTEXT)
Send Private Information Safely Over A Public Frame Relay Network:
News Release, pN/A
March 20, 1996
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 997
PUBLISHER NAME: Various
COMPANY NAMES: *Racal-Datacom Inc.
EVENT NAMES: *330 (Product information)
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *3662627 (Encryption/Decryption Equip)
INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)
NAICS CODES: 33429 (Other Communications Equipment Manufacturing)
SPECIAL FEATURES: COMPANY

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...encryptor is designed to provide an economical alternative to TI/E1 encryptors when used for the lower **speed** 56/64Kbps circuits that constitute the vast majority of frame relay connections. Protection for information in all...

...for optimum security. Under user control, some connections can be encrypted while others are not, saving the **cost** of installing encryption devices at frame relay sites that do not require security. The Racal Datacryptor Key...

...is assured of secure key distribution and control. Key changes can be performed automatically without operator intervention. **Cryptographic service** messages are authenticated using a secure protocol ensuring information integrity. For companies that require high volume data...

...character display provides valuable information on equipment status, including operating mode, active alarms and the date and **time** of important network events. The Data Link Connection Identifiers (DLCI's), which identify secured and unsecured virtual...

...powerup, be selected at the front panel or commence in response to Key Center commands at any **time** during operation. Available tests include

ROM/RAM, S-box, key parity, cipher feedback, checkword and memory. A...

12/5,K/19 (Item 3 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2003 The Gale Group. All rts. reserv.

02442183 Supplier Number: 43217641 (USE FORMAT 7 FOR FULLTEXT)
WEAK LINKS
InformationWeek, p26
August 10, 1992
ISSN: 8750-6874
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Tabloid; General Trade
Word Count: 2297
PUBLISHER NAME: CMP Publications, Inc.
COMPANY NAMES: *Corning Inc.; International Business Machines Corp.; Texas Instruments Inc.
EVENT NAMES: *980 (Legal issues & crime); 260 (General services)
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *4810000 (Telecommunication Services ex Broadcast); 3662192 (Facsimile Equipment); 3570000 (Office & Computing Machines); 3670000 (Electronic Components); 3210000 (Glass Products)
INDUSTRY NAMES: BUSN (Any type of business); CMPT (Computers and Office Automation); TELC (Telecommunications)
NAICS CODES: 5133 (Telecommunications); 33421 (Telephone Apparatus Manufacturing); 3359 (Other Electrical Equipment and Component Manufacturing); 3272 (Glass and Glass Product Manufacturing)
TICKER SYMBOLS: GLW; IBM; TXN
SPECIAL FEATURES: INDUSTRY; COMPANY

... Ratliffe. But that doesn't seem to concern most users. Although Kirkland, Wash.-based McCaw offers an **encryption** **service** that carries a $500 one- **time** hardware **cost** , plus a monthly service□charge□of $15 to $30, 'We don't have a lot of takers,' says Ratliffe.
'Not many of...

12/5,K/20 (Item 4 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2003 The Gale Group. All rts. reserv.

01308926 Supplier Number: 41536293
NEW SECURITY PRODUCTS ENCRYPT DATA AT HIGH SPEEDS
News Release, p1
Sept 5, 1990
Language: English Record Type: Abstract
Document Type: Magazine/Journal; Trade

ABSTRACT:
IBM today announced the industry's first integrated cryptographic feature and a new cryptographic architecture to help safeguard customers' vital information assets. The optional integrated cryptographic feature and its associated software enable customers to process large amounts of encrypted data up to four times faster than IBM's previous high-end processor encryption offering, resulting in a dramatic reduction in the **cost** of encryption. Also introduced today was a product providing enhanced security capability for workstations and personal computers, plus new "anti- virus" measures. The new high- **speed** Integrated Cryptographic Feature (ICRF) consists of a tamper-resistant Thermal Conduction Module (TCM) for

water-cooled models of Enterprise System/9000* processors and a key- entry unit. Integrated **Cryptographic Service** Facility/MVS (ICSF/MVS), a licensed program, is required for ICRF operation. Customers use the key-entry unit to enter master cryptographic keys into a secure key storage unit connected to the TCM by a tamper- resistant shielded cable. ICRF and ICSF/MVS also provide the high-performance bulk cryptography facility customers need to protect sensitive high- volume transaction processing applications. ICRF and ICSF/MVS support up to 1,000 IMS Fastpath transactions per second. This high performance is achieved by running ICRF operations at processor speeds rather than the channel speeds of previous offerings, using MVS/ESA* features and keeping cryptographic keys in processor storage rather than moving them between the processor and input-output devices. A single ICRF can support up to seven Processor Resource/Systems Management* (PR/SM)* partitions, each operating with its own unique master key. IBM today announced two measures to minimize the threat of harmful code, such as "viruses" and "worms," to customers' operations: -- IBM will offer an updated IBM Anti-Virus Product for DOS users to deal with more recently discovered viruses. -- IBM will also begin distributing software media, running on all platforms from workstations to the largest processors, in tamper- evident packaging as added protection against unauthorized modifications.

PUBLISHER NAME: Various
COMPANY NAMES: *International Business Machines Corp.
EVENT NAMES: *330 (Product information)
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *3662627 (Encryption/Decryption Equip); 7372691 (Data Encryption Software)
INDUSTRY NAMES: BUS (Business, General); BUSN (Any type of business)
NAICS CODES: 33429 (Other Communications Equipment Manufacturing); 51121 (Software Publishers)
TICKER SYMBOLS: IBM
SPECIAL FEATURES: COMPANY

ABSTRACT:
...faster than IBM's previous high-end processor encryption offering, resulting in a dramatic reduction in the **cost** of encryption. Also introduced today was a product providing enhanced security capability for workstations and personal computers, plus new "anti- virus" measures. The new high- **speed** Integrated Cryptographic Feature (ICRF) consists of a tamper-resistant Thermal Conduction Module (TCM) for water-cooled models of Enterprise System/9000* processors and a key- entry unit. Integrated **Cryptographic Service** Facility/MVS (ICSF/MVS), a licensed program, is required for ICRF operation. Customers use the key-entry...

12/5,K/21 (Item 1 from file: 553)
DIALOG(R)File 553:Wilson Bus. Abs. FullText
(c) 2003 The HW Wilson Co. All rts. reserv.

04050103 H.W. WILSON RECORD NUMBER: BWBA99050103 (USE FORMAT 7 FOR FULLTEXT)
Mass market solutions for mobile data.
AUGMENTED TITLE: general packet radio service
Clever, Michael
Telecommunications v. 33 no6 (June 1999) p. 40+
DOCUMENT TYPE: Feature Article ISSN: 0040-2494
LANGUAGE: English
COUNTRY OF PUBLICATION: United States
RECORD TYPE: Fulltext RECORD STATUS: Corrected or revised record
WORD COUNT: 2987

DESCRIPTORS:
Mobile communication systems; GSM (Global system for mobile communications)
SIC CODES: 4812

(USE FORMAT 7 FOR FULLTEXT)

TEXT:
... However, Seshu Madhavapeddy, senior product manager for Nortel Networks' wireless data products division, believes that low service **costs** will be essential for GPRS success. "It will be not **speed** alone, but **price** performance that matters. There is a market for wireless Internet services but even corporate intranet use is **price** sensitive, and this is at the high-end." As the **cost** of running traffic over a GPRS system is estimated to be one third that of a circuitswitched...

...the corporate intranet market for wireless operators." He envisions early service offerings to include VPNs, security and **encryption services** as well as customised services for large corporate accounts.
However, GPRS is also widely regarded as the...
?